RESEARCH IN FOCUS

Conceptual Ambiguity of International Norms on State Behaviour in Cyberspace

Zine Homburger
Leiden University
April 2019

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Abstract

The discussion about international norms for state behaviour in cyberspace gained prominence at an international level through the 2015 report of the United Nations Group of Governmental Experts (UNGGE). The motivation to adopt a concept of norms was rather pragmatic as it had proven difficult to engage in discussions on the applicability of international law within the UNGGE. It was considered easier to find consensus on voluntary and non-binding norms, yet neither the UNGGE nor the academic literature clarify what the concept of norms – especially as opposed to law – means. This conceptual ambiguity between law and norms leads to difficulties regarding legal predictability as well as the establishment of responsibility and possible responses to breaches of norms. This paper briefly showcases this ambiguity in the international debate and in literature as they pertain to international norms for state behaviour in cyberspace. Multilateral negotiations and other initiatives can present ways to clarify these two concepts. However, venue choice and the form of cooperation can also influence the legal relevance of negotiation outcomes. Finally, complementary action can help clarify what states consider obligations in cyberspace as well as violations. But what action a state can take in response to a malicious cyber activity depends on the act being categorised as a violation of law or merely a violation of voluntary non-binding norms.

Key points

- The creation of the concept of voluntary, non-binding norms – as opposed to law – has led to conceptual ambiguity in the regulation of state behaviour in cyberspace.
- Conceptual ambiguity can lead to legal uncertainty and makes the determination of responsibility more challenging.
- Multilateral meetings and exchanges of ideas and interests play an important role in clarifying those ambiguities. But they can also further blur these two concepts.
- Additionally, complementary action can help clarify what states consider obligations in cyberspace as well as violations. However, the action that a state can take in response to malicious cyber activity highly depends on whether that activity is categorised as violating a law or merely breaching a norm.
- The debate over which norms states should adopt, for all the disagreement and back-and-forth, will prove a necessary part of the process; in the end, it will increase clarity, and therefore security, in cyberspace.

1. Introduction

Amid rising concern over threats to internationa l peace and security from the use of ICTs, states agreed to discuss the regulation of state behaviour in cyberspace. The specific discussion about *norms* for responsible state behaviour in cyberspace has emerged from the United Nations Group of Governmental Experts' (UNGGE) findings on developments in the field of information and telecommunications in the context of international security.[1] The first resolutions establishing the UNGGE process, as well as UNGGE reports in 2010 and 2013, use the term *norm* interchangeably with rules and principles; they also point towards a concept with legally binding character.[2] Furthermore, the UNGGE in 2013 agreed on the general applicability of international law to state behaviour in cyberspace.[3] However, the difficulty of clarifying the role of international law with regard to state behaviour in cyberspace became evident through the outcome of the UNGGE in 2017, which was unable to agree on a consensus report. Back in 2015, the UNGGE report had clearly introduced the terminology of *voluntary, non-binding norms* for the first time. To establish a legally non-binding framework for the discussion was a pragmatic choice, as it had become evident that consensus on "new" binding international law would be as difficult to achieve as consensus on concrete terms for application of existing international law. However, it did not contribute to the clarification of the concepts envisioned by states to govern behaviour in cyberspace. The clear distinction between norms and law, as per the 2015 report of the UNGGE, makes an examination of exactly these concepts – norms as opposed to law – necessary. Indeed, if norms were international law, states would be bound by them. A violation (negative obligations) or a non-fulfillment (positive obligations) would lead to legal responsibility and the possibility of countermeasures by injured states. If norms were purely voluntary, the enforcement mechanisms offered by international law would not be applicable. Furthermore, political measures, such as 'naming and shaming', might be more effective when brought about by a violation of international law rather than a violation of voluntary norms. Explicit knowledge of the legal relevance of certain norms would not only lead to legal predictability, but clarification about which actions lead to legal responsibility.

"

Neither the academic debate over norms for state behaviour in cyberspace nor international law have a coherent definition of norms, whether as a legally binding concept or a non-legally binding and voluntary concept.

2. Conceptual Ambiguity

Neither the academic debate over norms for state behaviour in cyberspace nor international law have a coherent definition of norms, whether as a legally binding concept or a non-legally binding and voluntary concept. The 2015 UNGGE report, for example, introduced the following as a recommendation for a voluntary, non-binding norm: *"States should not knowingly allow their territory to be used for*

[1] For an overview, see "Developments in the field of information and telecommunications in the context of international security." United Nations Office for Disarmament Affairs. Accessed 10 December 2018. https://www.un.org/disarmament/topics/informationsecurity/

[2] United Nations, General Assembly, "Developments in the field of information and telecommunications in the context of international security," para. 4, UN Doc. A/RES/66/24 (13 December 2011); United Nations, General Assembly, "Developments in the field of information and telecommunications in the context of international security," para. 15, UN Doc. A/RES/71/28 (9 December 2016); United Nations, General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", para. 16, UN Doc. A/65/201 (30 July 2010); United Nations, General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,", para. 4, UN Doc. A/68/98 (24 June 2013).

[3] United Nations, General Assembly, UN Doc. A/68/98 (24 June 2013), para. 19.

internationally wrongful acts using ICTs".[4] From the language used to the foundational concept of this norm, it resonates with the due diligence principle in international law.[5] This is a legal principle from which certain obligations for state behaviour derive. It is based on the fundamental principle of state sovereignty and anchored in the Corfu Channel judgment of the International Court of Justice (ICJ). Here, the court stipulated that every state has the obligation *"not to allow knowingly its territory to be used for acts contrary to the rights of other States"*.[6] Subsequent ICJ rulings confirmed that this principle represented customary international law.[7] It is closely connected to the principle of sovereignty and the duty to respect the territorial sovereignty of other states.[8] The 2015 UNGGE report agrees that state sovereignty "*and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory*".[9] Therefore, it could be argued that the group deems the principle of due diligence applicable to the use of ICTs.[10] Additionally, the group acknowledges that international law demands that states not let their territory be used for international wrongful acts.[11] This seems to contradict the principle of norms being explicitly voluntary and non-binding and is just one example of labeling a norm voluntary even when it is strongly connected to legally binding principles of international law.

Further uncertainty arises due to the similar function of norms and law. Similar to law, norms provide a basis for evaluating behaviour and labeling activities as appropriate or inappropriate. Whereas reputational impact might be stronger if a state violates international law, states can also be called out for violations of agreed-upon norms. Those reactions could compose lawful measures, also known as retorsion. The United States, for example, imposed sanctions against Russia for having hacked the US elections in 2016 as well as against North Korea in response to several malicious cyber activities.[12] When a state argues that a cyber incident is not only a breach of a non-binding norm but of international law, more forceful forms of consequences become possible. When international law is violated, an injured state can take countermeasures – measures which would otherwise be in violation of international law themselves.[13] Such measures can be more severe than retorsions and may, therefore, pull the perpetrator state towards greater compliance. Clarification of the ambiguity between laws and norms is therefore necessary.

In academic literature, the term *norm* is often defined as a "*standard of appropriate behavior for actors with a given identity*".[14] This definition describes norms as social constructs and does not mention

[4] United Nations, General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", para. 13(c), UN Doc. A/70/174 (22 July 2015).
[5] For an extensive discussion of the norm, see Liisi Adamson, "Recommendation 13(c)," in *Voluntary, Non-Binding Norms for Responsible State Behavior in the Use of Information and Communications Technology: A Commentary* (New York: United Nations Publications, 2017), Civil Society and Disarmament: iii-270, pp. 49-77.
[6] ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment, ICJ Reports 1949, p. 4;22.
[7] ICJ, *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment, ICJ Reports 2010, p. 14, para. 101; with regard to international environmental law: ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996, 226; *ICJ Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)* and *Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)*, Judgment, ICJ Reports 2015, 665, para. 104.
[8] This principle was confirmed by the ICJ in ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Reports 1986, 14, para. 213.
[9] United Nations, General Assembly, UN Doc. A/70/174 (22 July 2015), para. 27.
[10] For a discussion of the application of the due diligence principle in cyberspace see Rule 6 "Due Diligence (general principle,", in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. M. N. Michael Schmitt (Cambridge University Press, 2017), 30-43.
[11] United Nations, General Assembly, UN Doc. A/70/174 (22 July 2015), para. 28(e).
[12] U.S. Department of the Treasury, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks", Press Release (March 15, 2018), Accessed 10 December 2018. https://home.treasury.gov/news/press-releases/sm0312; US Department of the Treasury, "Treasury Targets North Korea for Multiple Cyber Attacks", Press Release (September 6, 2018), Accessed 10 December 2018. https://home.treasury.gov/news/press-releases/sm473.
[13] For the application of countermeasures, see Art 49, International Law Commission (ILC), *Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries* in United Nations, *Yearbook of International Law*, Vol. II, Part Two (2001).
[14] See inter alia definitions used by Martha Finnemore & Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52 (1998): 887-917, p. 891.

whether they have legal relevance or not. Indeed, many international relations scholars do not differentiate between international norms and international law. This is because their primary concern is not the investigation of applicable and binding law. If a distinction is made, norms are referred to as social norms distinct from law.[15] This distinction is especially valuable considering that in national or domestic orders, norms are held and enforced by societies, whereas law is imposed by a higher sovereign.[16] In an international system in which states are regarded as equal sovereigns, no such legislative authority exists. Hence, law is created - and enforced – among the states, similar to how social norms would evolve in a domestic system.

Art. 38 of the ICJ statute[17] is often referred to when investigating the sources of international law. According to art. 38, the primary sources of international law include international conventions, international custom contained of practice accepted as law and general principles of international law. The article does not mention the concept of norms. Nevertheless, this does not mean that international law treats norms as a non-legal concept. The ILC seems to refer to norms as an encompassing concept for rules as well as principles.[18] Accordingly, rules are norms of a lower degree of abstraction than principles.[19] As such, norms are a legal concept and can describe legally binding obligations. More interestingly, the term norm is used in international law to refer to *ius cogens*. In the Vienna Convention on the Law of Treaties[20], the term *norm* appears in art. 53 as well as art. 64, which deal with peremptory norms of international law. Art. 53 stipulates that "*a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted*". An example of *ius cogens* norms are the prohibition of torture or the prohibition of genocide. This means, in international law, the term *norm* can indeed refer to a legally binding concept. Even if one were to assume that norms are not a legally binding concept, they may become legally binding over time. Identifying norms could be a first step toward identifying customary international law. Customary international law is comprised of a common practice by states plus a sense of legal obligation that is often referred to as *opinio juris*.[21] Contrary to established customary international law, norms might miss the element of being accepted as already established law even though they reveal a standard of what is considered appropriate and what is not. Continuous practice and reaffirming such norms could, over time, see certain norms reach the status of customary international law.

The definition of norms used in the UNGGE mirrors to a certain extent the definitions given within the academic literature. According to the UNGGE's 2015 report, "*norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States*".[22] Rather than settling on a single concept, this definition states that norms can be expectations as well as standards. This definition also reflects the need for norms to be shared among actors, as is indicated by the words "international community". At the same time, this definition includes an expectation as well as an evaluation of behaviour based on a norm. Like the definition in academic literature, the UNGGE's definition does not indicate the legal relevance of a norm. Additionally, earlier UNGGE reports do not draw a clear-cut line between norms and international law. The body's first report in 2010 states that "*existing agreements include norms relevant to the use of ICTs by States*".[23] The Vienna Convention on the Law of Treaties uses the term

[15] See, e.g., Cass R. Sunstein, "Social Norms and Social Role," *Columbia Law Review* 96, no. 4 (1996):903–68; see Amy Gurowitz, "Mobilizing International Norms: Domestic Actors, Immigrants, and the Japanese State," *World Politics* 51, No. 3 (1999): 413-445.
[16] See, e.g., Lawrence Lessig, *Code 2.0.*, 2nd ed. (New York: Basic Books, 2006).
[17] United Nations, *Charter of the United Nations and Statute of the International Court of Justice* 1945, UN Treaty Series 1, XVI [hereinafter ICJ Statute].
[18] See International Law Commission (ILC), *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law*, UN Doc. A/CN.4/L.682 (13 April 2006), p. 28.
[19] Ibid.
[20] United Nations, *Vienna Convention on the Law of Treaties*, 1155 UN Treaty Series (23 May 1969), p. 331 [hereinafter VCLT].
[21] See ICJ statute, Art. 38.
[22] United Nations, General Assembly, UN Doc. A/70/174 (22 July 2015), para. 10.
[23] United Nations, General Assembly, UN Doc. A/65/201 (30 July 2010), para. 16.

agreement to define a treaty that is concluded between states in written form and governed by international law.[24] As part of an existing agreement, norms would thus be international law; they would therefore have a legal character and not be purely voluntary. The same report states that additional norms could be developed with the special features of cyberspace in mind. Should those developed norms be entailed in a treaty, they would represent binding international law.[25] Nevertheless, if those norms were not adopted in such a manner, they might have no legally binding character. Only the 2015 UNGGE report introduces norms as voluntary and non-binding and recommends 11 such norms. However, upon examination of the proposed norms, it can be established that they build upon international law and could arguably represent applicable international law.[26] By labeling them as voluntary and non-binding, the Group of Governmental Experts clarified which basic principles of international law might not be directly applicable to state behaviour in cyberspace. In doing so, they seemed to defy their own agreement that international law is generally applicable to cyberspace. This leads to uncertainty and legal unpredictability, which can itself have an impact on states' activities and affect further development of a normative framework for state behaviour in cyberspace.

3. Multilateral Negotiations and Other Initiatives

Multilateral negotiations and an exchange of ideas on international platforms can help clarify identified uncertainties and ambiguities. Furthermore, they are important avenues for exchanging ideas and contributing to the further development of international law. For this reason, states mandated the UNGGE in the realm of the First Committee of the UNGA. Those meetings, held by a Group of Governmental Eperts, were highly influenced by the different states' approaches to cybersecurity governance. However, one point of criticism against the UNGGE process is its lack of transparency in member selection for joining the group. Furthermore, the non-agreement between members of the 2017 UNGGE diminished faith in this form of interaction. Working within the UN framework, the group contributes to one of the purposes listed in art. 1(3) of the UNC, to wit: "international co-operation in solving international problems". Furthermore, the group is mandated by the UNGA. According to art. 13(1)(a), the UNGA is tasked with contributing to international cooperation and the further development of international law and its codification. Consequently, even though resolutions of the General Assembly (or of one of its mandated bodies) are not legally binding, they are relevant for the development of international law and can lead to clarification of existing and codification of new international law. Mandating a venue under the UNGA may therefore facilitate the development of international law concerning state behaviour in cyberspace. In November 2018, two resolutions with different suggestions regarding the ongoing process at the United Nations were introduced within the First Committee.[27] The discussion about the appropriate platform going forward mirrors the debate over how cyberspace should be governed. Based on the Russian Federation's proposal, the UNGA adopted a resolution on "*developments in the field of information and telecommunications in the context of international security*".[28] This resolution establishes an open-ended working group under the auspices of the United Nations to further develop norms, rules and principles of responsible behaviour of states and their implementation.[29] The purpose of the working group is to negotiate security in information and

[24] VCLT, Art. 2(a).
[25] Ibid.
[26] *Voluntary, Non-Binding Norms for Responsible State Behavior in the Use of Information and Communications Technology: A Commentary* (New York: United Nations Publications, 2017), Civil Society and Disarmament: iii-280, pp. 49-77.
[27] United Nations, "First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct," Meeting Coverages and Press Releases, GA/DIS/3619 (8 November 2018). Accessed 13 December 2018. https://www.un.org/press/en/2018/gadis3619.doc.htm; for the consideration in the UNGA plenary see, United Nations, "General Assembly Adopts 67 Disarmament Drafts, Calling for Greater Collective Action to Reduce Arsenals, Improve Trust amid Rising Global Tensions," Meetings Coverages and Press Releases, GA/1209 (5 December 2019). Accessed 13 December 2018. https://www.un.org/press/en/2018/ga12099.doc.htm
[28] See United Nations, General Assembly, "Developments in the field of information and telecommunications in the context of international security", UN Doc. A/RES/73/27 (11 December 2018).
[29] Ibid, para 5.

communications technologies.[30] Due to criticism against the former UNGGEs, this working group is supposed to be more democratic, inclusive and transparent.[31] Almost simultaneous to the Russian proposal, the United States tabled a resolution on "advancing responsible State behavior in cyberspace in the context of international security". That resolution establishes a Group of Governmental Experts on the basis of equitable geographical distribution, which is supposed to promote common understandings and implementation with regard to norms, rules and principles of responsible behaviour of States.[32] This mandate is similar to that of the working group suggested by Russia, but its concepts and the language used are more similar to previous resolutions establishing UNGGEs and UNGGE reports. While ongoing dialogue within the United Nations is certainly to be welcomed, the groups' similar mandates might actually lead to more ambiguity regarding applicable international law and norms. Furthermore, despite both bodies being created transparently and with equitable geographical distribution in mind, many states won't be able to contribute to both bodies in a meaningful way due to a lack of resources.

"

Multilateral negotiations and an exchange of ideas on international platforms can help clarify identified uncertainties and ambiguities. Furthermore, these are important avenues for exchanging ideas and contributing to the further development of international law.

As an alternative to agreement at a UN level, states have increasingly developed initiatives among like-minded countries.[33] These approaches could, however, result in a fragmentation of norms and law. Therefore, they may not be an effective solution to the governance of a global cyberspace. If each group of like-minded states agrees on its own norms and bilateral or regional law, the normative framework could get rather complicated. An example is the Budapest Convention[34], which started as a "like-minded approach". Today several states that are not members of the Council of Europe (CoE) have ratified the Convention.[35] Nevertheless, the Russian Federation, as a member of the CoE, as well as other members of the Shanghai Cooperation Organization, such as China, have not ratified the Budapest Convention. The same is true for the Code of Conduct promoted by the Shanghai Cooperation Organization (SCO), which is not supported by Western states. These separate developments could endanger not only the reach of those instruments but also, in the long run, the fundamental norm of ensuring an open, free and secure internet. The ideological divide between these groups of countries is also reflected in the current discussion over a continuation of a United Nations-led process.

In addition to cooperation within the realm of international organisations, an increasing amount of non-state initiatives and platforms are forming to discuss the international regulation of state behaviour in cyberspace. Because they are primarily non-governmental, these avenues may not directly contribute to international regulation as agreed upon among states. Nevertheless, these initiatives are helping keep discussions alive, especially when intergovernmental dialogues fail to lead to any meaningful outcomes. Furthermore, non-state actors can influence states' positions by acting as norm-entrepreneurs.[36] Microsoft and the Global Commission on the Stability in Cyberspace, for example,

[30] Ibid.
[31] Ibid.
[32] Ibid, para. 3.
[33] As it was suggested by some states after the UN GGE did not agree on a consensus report in 2017, see J. Nye, Normative Constraints on Cyber Arms, in: Fen Osler Hampson & Michael Sulmeyer (eds), "Getting beyond Norms: New Approaches to International Cyber Security Challenges," Special Report (Centre for International Governance Innovation, 2017): vii-35, p. 21.
[34] Council of Europe, *Convention on Cybercrime*, European Treaty Series 185 (23 November 2001).
[35] "Chart of signatures and ratifications of Treaty 185," Convention on Cybercrime. Status as of 14/12/2018. Council of Europe. Accessed 14 December 2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=wPXNn2kz.
[36] For an introduction to the concept of norm entrepreneurship see Martha Finnemore & Kathryn Sikkink "International Norm Dynamics and Political Change."

contribute to the discussion by proposing new norms which they deem important for the regulation of state behaviour in cyberspace. Microsoft promotes a Digital Geneva Convention for Peacetime which includes norms on the non-proliferation of cyber weapons as well as refraining from hacking personal accounts or using information and communication technology to steal intellectual property.[37] Similarly, the Global Commission promotes new norms within its Singapore Norm Package.[38] These norms include the responsibility of creating a vulnerability equities process and enacting measures for basic cyber hygiene.[39] The norm package primarily includes norms addressed towards states as well as non-state actors.

However, those initiatives and the non-state actors behind them are often not completely detached from state institutions. The Netherlands, France, Singapore and Estonia, for example, are partners and sponsors of the GCSC.[40] Additionally, many commissioners of the GCSC have worked formerly for a government.[41] These initiatives can influence not only state positions, they can also take up state initiatives. The GCSC, for instance, is promoting the norm of protecting the public core of the internet[42]. This was originally proposed by the Netherlands during discussions at the UN but failed to gain the support of all UNGGE members. Now, the GCSC has taken up the initiative in order to gain support for the norm. An example of a joint initiative between non-state actors and governments is the Paris Call for Trust, which several private sector actors, states and other organisations have signed.[43] It reaffirms the application of international law and norms to state behaviour in cyberspace.[44] Furthermore, it lays down the agreement for cooperation in order to fulfill several goals contributing to stability in cyberspace, one of which is the promotion of the acceptance and implementation of international norms.[45]

“

It seems that until now, these initiatives have adopted language referring to international law and norms on responsible state behaviour in cyberspace without actually contributing to any clarification of the legal relevance of these two distinct concepts.

This magnitude of venues and initiatives – whether they are intergovernmental or comprised of states and non-state actors – shows the apparent importance of the subject matter. Whereas those forms of interaction can be valuable to clarify existing concepts and ambiguities, they can also further confuse things. It seems that until now, these initiatives have adopted language referring to international law and norms on responsible state behaviour in cyberspace without actually contributing to any clarification of the legal relevance of these two distinct concepts.

[37] “A Digital Geneva Convention to protect cyberspace,” Microsoft Policy Papers. Microsoft. Accessed 13 December 2018. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.
[38] Global Commission on the Stability of Cyberspace, “Norm Package Singapore,” November 2018. Accessed 13 December 2018. https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.
[39] Global Commission on the Stability of Cyberspace, “Norm Package Singapore,” p. 12-14; p. 16-18.
[40] “About.” Global Commission on the Stability of Cyberspace. Accessed 12 December 2018. https://cyberstability.org/about/ (12.12.2018).
[41] See, e.g., Marina Kaljurand, Former Minister of Foreign Affairs of Estonia and Commissioner of the GCSC. “Marina Kaljurand.” Global Commission on the Stability of Cyberspace. Accessed 12 December 2018. https://cyberstability.org/commissioners/marina-kaljurand/; Michael Chertoff formerly working for the US Department of Homeland Security and as a Commissioner to the GCSC. “Michael Chertoff.” Global Commission on the Stability of Cyberspace. Accessed 12 December 2018. https://cyberstability.org/commissioners/michael-chertoff/
[42] Global Commission on the Stability of Cyberspace, “Call to Protect the Public Core of the Internet,” New Delhi, November 2017. Accessed 12 December 2018. https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf
[43] France Diplomatie, “Appel de Paris pur la confiance et la sécurité dans le cyberspace,” 12 November 2018. Accessed 13 December 2018. https://www.diplomatie.gouv.fr/IMG/pdf/14_soutien_appel_paris_cle093316.pdf
[44] France Diplomatie, “Paris Call for Trust and Security in Cyberspace,” 11 December 2018, para 3-5. Accessed 13 December 2018. https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf
[45] Ibid.

4. Complementary Action

Slow progress within the UN and increasing cyber incidents call in question the reliance on long-lasting, difficult negotiations at a UN level or within other venues. This makes additional complementary action necessary, as emphasized by the Cyber Diplomacy Toolbox discussed within the EU.[46] In a decision by the Council of the European Union, the EU signals that it is likely to employ consequences for malicious cyber activities.[47] Those actions can contribute to the implementation of agreed upon norms as they can deter potential perpetrators.[48] Furthermore, those actions – state activities and state practice – can contribute to the clarification of the current normative framework. It is necessary to bear in mind that norms and law are not only created through international negotiations, such as within the UNGGE or bi- or plurilateral processes like the SCO or EU; law and norms are also heavily influenced by state practice which itself is often based on a sense of legal legitimacy. An example is the attribution of cyber incidents to certain states, followed by the imposition of sanctions for those incidents – as the US did in the cases of Russia and North Korea.[49] Attribution in international law follows narrow standards entailed in the Draft Articles on State Responsibility,[50] but the political attribution of cyber incidents might not meet these legal standards.[51] In the long run, however, this practice could contribute to lowering the standard of legal attribution for cyber incidents.[52] Regarding the creation of laws and norms through practice, inaction by states matters as well. Not clarifying which action is considered right, and which wrong, could be perceived as tacitly agreeing that some behavior is acceptable.[53] An example of this is intelligence gathering outside the realm of economic espionage; to actively engage in it without clarifying that states consider it illegitimate could be seen as tacit approval and contribute to a norm that allows such conduct. Therefore, it is important to bear in mind that states can unilaterally influence the creation of norms and laws governing behaviour in cyberspace.

An example of such complementary action is the imposition of sanctions by the US, as mentioned above.[54] Also low-level actions, such as calling out behaviour considered a violation of international law as well as political attribution, help to clarify what conduct is deemed acceptable and what is not. In a speech delivered by the UK ambassador to the Netherlands, Peter Wilson, on behalf of Europe Minister Alan Duncan, the UK and the Netherlands condemned the cyberattacks against the Organisation for the Prohibition of Chemical Weapons (OPCW). In doing so, he emphasized the importance of exposing such behaviour and combining it with possible sanctions.[55] Furthermore, the UK called out the Russian

[46] Council of the European Union, "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")", 9916/17, Brussels (7 June 2017). Accessed 13 December 2018. http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf; for a discussion see Erica Moret and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?," EU Institute for Security Studies, July 2017. Accessed 13 December 2018.

[47] Council of the European Union, "Draft Council Conclusions", para. 4.

[48] Ibid.

[49] See US Department of the Treasury, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks." Press Release (March 15, 2018). Accessed 10 December 2018. https://home.treasury.gov/news/press-releases/sm0312; US Department of the Treasury, "Treasury Targets North Korea for Multiple Cyber Attacks." Press Release (September 6, 2018). Accessed 10 December 2018. https://home.treasury.gov/news/press-releases/sm473.

[50] Art 4-11, International Law Commission (ILC), *Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries*.

[51] This concern is also addressed in United Nations, General Assembly, UN Doc. A/RES/73/27 (11 December 2018), para. 1-2.

[52] Peter Stockburger, "Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents" in *9th International Conference on Cyber Conflict Defending the Core* (2017), ed. by H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Tallinn: NATO CCD COE Publications 2017), 149-163.

[53] For a discussion of tacit consent, see Doris König, "Tacit Consent/Opting Out Procedure" in Max Planck Encyclopedia of Public International Law (January 2013).

[54] For a discussion on tools to deter malicious cyber activities see Kathleen Claussen, "Beyond norms: using international economic tools to deter malicious state-sponsored cyber activities" *Temple International & Comparative Law Journal* 32, vol. 2 (Summer 2018): 113-127.

[55] Foreign & Commonwealth Office and Peter Wilson CMG, "Minister for Europe statement: attempted hacking of the OPCW by Russian military intelligence." (4 October 2018). Accessed 13 December 2018.

military intelligence service (GRU) in early October for several cyberattacks – the UK's National Cyber Security Center (NCSC) had attributed several cyberattacks to the GRU in 2016, 2017 and 2018.[56] At the same time, the NCSC clarified that it considered the attacks a violation of international law.[57] Foreign Secretary Jeremy Hunt stated in this context that the GRU operates "*without regard to international law or norms*".[58] While on the one hand, this statement is a valuable step towards the clarification of acceptable behaviour in cyberspace, it again emphasizes the ambiguous distinction between international law and norms.

5. Conclusion

The current debate on responsible state behaviour in cyberspace among governments, academia and other stakeholders focuses on three major points: **1)** the promotion of new norms and the application of existing international law; **2)** the implementation of norms and law; and **3)** the facilitation of dialogue to continue developing the topic. Bodies at the United Nations are currently mandated to further clarify the application of international law and norms. Other actors, such as the US, favour acting upon existing norms and implementing international law, in line with the notion of complementary action. In this regard, the EU is also eager to act within the limits of international law as expressed by the Cyber Diplomacy Toolbox. And finally, others actors, for their part, are engaged in determining how to proceed with the process of facilitating international dialogue – or maybe even official multilateral negotiations – on responsible state behaviour in cyberspace. Underlying all three processes is the conflation of international norms and international law on responsible state behaviour in cyberspace. By separating norms from law on the basis that the former are voluntary and non-binding, actors create a concept that is flexible and that could be more conducive to agreement than law would be. However, considering the content of those norms, a clear distinction from international law that already exists and is arguably applicable is sometimes impossible to make. Therefore, despite the apparent clear distinction in the language of those voluntary, non-binding norms from legally binding law, this development has led to conceptual ambiguity. That ambiguity, in turn, has an impact on state activities and on further development of a normative framework for state behaviour in cyberspace.

Multilateral meetings and exchanges of ideas and interests play an important role in clarifying those ambiguities and contribute to further development. In lieu of diverging state interests, two future UN-based dialogues are being established at the moment. This process reaffirms the difficulty of reaching agreement on the regulation of state behaviour in cyberspace. Finally, complementary action can contribute to clarifying what states consider obligations in cyberspace and what they consider violations. However, what action a state can take in response to malicious cyber activity highly depends on the categorisation of the act into an internationally wrongful act or just an unfriendly but legal act; in other words, was the act a violation of international law or only a violation of voluntary non-binding norms? In conclusion, the discussion on international law and norms as well as the effort to agree on venues to discuss those topics and the consideration of complementary action is influenced to a certain extent by the ambiguity between laws and norms. In the end, all three concerns and efforts will be necessary and will hopefully determine how to increase clarity – and therefore stability – in cyberspace.

https://www.gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence.

[56] National Cyber Security Centre, "Reckless campaign of cyber attacks by Russian military intelligence service exposed." (4 October 2018). Accessed 13 December 2018. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

[57] National Cyber Security Centre, "Reckless campaign of cyber attacks", Foreign Secretary Jeremy Hunt: „These attacks have been conducted in flagrant violation of international law, have affected citizens in a large number of countries, including Russia, and have cost national economies millions of pounds."

[58] Ibid.

Annex: Norms adopted by the UN GGE and their foundation in international law

This section is based on United Nations Office of Disarmament Affairs, *Voluntary, Non-Binding Norms for Responsible State Behavior in the Use of Information and Communications Technology: A Commentary*, (New York: United Nations Publications, 2017).

Legal relevance of the general work of the UNGA

The United Nations Group of Governmental Experts (UN GGE) recommending voluntary, non-binding norms on responsible state behavior in cyberspace was mandated by the United Nations General Assembly (UNGA). In general, processes and agreements generated through the UNGA are legally non-binding. Therefore, it is not surprising that the UN GGE only recommended voluntary, non-binding norms. Nevertheless, a closer look at the general framework within which the UNGA operates, shows that its work and the work of its committees might be legally relevant. According to art. 1(1) and art. 1 (2) UN Charter (UNC), the purposes of the UN are inter alia the peaceful settlement of international disputes and the cooperation in solving international problems. According to the UNC, the mandate of the UNGA is *inter alia* to initiate studies and make recommendations as well as "encourage the progressive development of international law" (Art. 13(1)(a) UNC) for those ends. This means that the UNGA – different to the United Nations Security Council (UNSC) – cannot create legally binding rules but it, nevertheless, can contribute to the development of international law. Furthermore, a closer look at the norms recommended by the UN GGE shows that those norms build on existing international law and general principles of the international legal order. To label them as voluntary, non-binding does not acknowledge their foundation in international law.

Norms and their foundation in international law

Norm

> [...] States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security
>
> *'Norms', para. **13(a)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

Cooperation is an essential element for the creation of international law.

The **Friendly Relations Declaration** which acquired partly customary law status states the following: "States have the duty to co-operate with one another (...) in the various spheres of international relations, in order to maintain international peace and security."

Examples of special regimes which entail a duty to cooperate

- International Convention for the Regulation of Whaling (ICRW): The ICJ stated in its judgment "Whaling in the Antarctic" with regard to the ICRW: "The Court however observes that the States parties to the ICRW have a duty to co-operate with the IWC and the Scientific Committee and thus should give due regard to recommendations calling for an assessment of the feasibility of non-lethal alternatives" (*Whaling in the Antarctic (Australia* v. *Japan: New Zealand intervening), Judgment, I.C.J. Reports 2014*, p. 226, para. 83);
- The international climate protection regime entails the duty to cooperate based on the United Nations Framework Convention on Climate Change (UNFCCC)
  - Art. 4(1)(c) UNFCCC: All Parties (...) shall (...) cooperate in the development, applications and diffusion, including transfer of technologies, practices and processes that control, reduce or prevent anthropogenic emissions (...);
  - Art. 4(1)(e) UNFCCC: All Parties (...) shall (...) cooperate in the conservation and enhancement, as appropriate, of sinks and reservoirs of all greenhouse gases (...).

The norm invokes the recommendation to prevent harmful practices

- The prevention of harmful consequences for other states falls within the realm of the **due diligence principle** (see **norm c**);
- Within the Constitution of the **International Telecommunication Union (ITU)**, a duty to prevent Harmful interference exists entailed in special provisions for Radio:
  - Art. 45: All stations (...) must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States (...).

The obligation to **prevent transboundary harm** is entailed in the ILC Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities (this regime is not applicable but shows the principle exists in other fields of international law):

- Art. 3: The State of origin shall take all appropriate measures to prevent significant transboundary harm or any event to minimize the risk thereof;
- Art. 2(c): "Transboundary harm" means harm caused in the territory of or in other places under the jurisdiction or control of a State other that the State of origin, whether or not the States concerned share a common border.

Norm

> [...] States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

*'Norms', para. **13(b)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

This norm relating inter alia to the response to cyber incidents is connected to the **general principle of the peaceful settlement of international disputes.**

- Art. 2(3) UNC: All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.

Attribution and the imposition of **consequences** for state activities is generally governed by the law of state responsibility as entailed in the Draft Articles on State Responsibility.

- Standards of attribution to a state are entailed in art. 4-11of the ILC Draft Articles on State Responsibility;
- Standards for the invocation of responsibility by an injured state and the imposition of consequences for internationally wrongful acts are entailed in art. 42-54 ILC Draft Articles on State Responsibility.

Norm

> [...] States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

*'Norms', para. **13(c)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

Due diligence principle

- The principle of due diligence is based on the principle of state sovereignty (see **norm h**);
- The principle of due diligence is affirmed by the ICJ in the Corfu Channel Case 1949: "The obligations incumbent upon the Albanian authorities consisted in **notifying**, for the benefit of shipping in general, the existence of a minefield in Albanian territorial waters and in **warning** the approaching British warships of the imminent danger to which the minefield exposed them" (p.22). This is based "on certain general and well-recognized principles, namely : (...) **every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States**." (p. 22). (Corfu Channel case, Judgment of April 9th, 1949: I.C.J . Reports 1949, P. 4.);
- The ICJ confirmed the principle again in its Pulp Mills Case (2010) in para. 101: "The Court points out that the principle of prevention, as a customary rule, has its origins in the **due diligence** that is required of a State in its territory. It is "**every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States" (...)**. A State is thus obliged to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State. This Court has established that this obligation "is now part of

the corpus of international law relating to the environment" (...)." (Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 14);

- In the Judgment Nicaragua v. Costa Rica (2015), the ICJ confirms the principle as part of customary international law again in para. 104 (Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports 2015, p. 665).

UN GGE report 2015 A/70/174, 'Chapter VI: How international law applies to the use of ICTs'

- Para. 26: In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of disputes by peaceful means (...) refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State (...);
- Para. 27: State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.
- Para 28: (...) the present Group offers the following non-exhaustive views on how international law applies to the use of ICTs by States:
  - **a)** States have jurisdiction over the ICT infrastructure located within their territory;
  - **b)** In their use of ICTs, states must observe among other principles of international law, state sovereignty, sovereign equality (...);
  - **e)** States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts.

Norm

> States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect

*'Norms', para. **13(d)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

Mutual legal assistance/Cooperation in criminal matters

- The Budapest Convention of the Council of Europe (Et No. 185) establishes in principles relating to international cooperation in criminal matters.

Existing Treaties on assistance/cooperation in combating transnational crime or terrorist financing

- UN Transnational Organised Crime Convention: art. 7(4) (regarding money laundering); art. 13 (international cooperation for purposes of confiscation), art. 16 (extradition), art. 20 (special investigative techniques), art. 26 (measures to enhance cooperation with law enforcement authorities);
- EU Convention on Mutual Legal Assistance;

- Convention on the Prevention of Terrorism Financing.

Norm

> States in ensuring the secure use of ICTs, should respect Human Rights Council resolution 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy and the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

*'Norms', para. **13(e)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

Human Rights obligations in international law

- Universal declaration of human rights: art. 19 (freedom of expression); art. 12 (right to privacy);
- ICCPR: art. 19 (freedom of expression); art. 17 (right to privacy);
- ECHR: art. 8 (right to privacy) and art. 10 (freedom of expression).

UN GGE report 2015 A/70/174, 'Chapter VI: How international law applies to the use of ICTs'

- Para. 26: In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: (…) respect for human rights and fundamental freedoms (…);
- Para 28 (b): (…) States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms.

Norm

> A state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure to provide services to the public.

*'Norms', para. **13(f)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

When a state acts against its international legal obligations, it commits an international wrongful act.

- Art. 2 of the **ILC Draft Articles on State Responsibility** define an international wrongful act as consisting of an action or omission attributable to a state which constitute a breach of an international obligation (**see norm b** for attribution).
- An obligation of a state under international law can arise from treaty obligations as well as customary international law.
- The norm assumes that the intentional damaging of critical infrastructure to provide services to the public constitutes a breach of obligations under international law. Therefore, the norm makes a legal categorization even though it is assumed to only be a recommendation for a non-legally binding norm.

The terminology of "knowingly supporting" resonates with the due diligence principle in international law (see **norm c**).

Norm

> States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

*'Norms', para. **13(g)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

This norm is phrased as a positive obligation. Whereas negative obligations demand a state to refrain from certain actions, positive obligations demand a state to proactively ensure certain rights or situations. To protect infrastructure within a state's own territory is not based on an existing international law obligation. It connects, however, to the principle of prevention and due diligence.

Norm

> States should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

*'Norms', para. **13(h)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

Assistance upon request can be seen as a form of **cooperation** (see **norm a**).

The **principle of sovereignty** in international law ensures the territorial integrity of a state and the protection of other states interfering with this integrity.

- Art. 2 UNC:
  1) The Organization is based on the principle of the sovereign equality of all its Members.
  4) In All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.
- Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14:
  - para. 212: The court stresses the basic legal concept of State sovereignty in customary international law.
  - para. 213: the court reaffirms he duty of every State to respect the territorial sovereignty of others.

- PCIJ, S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7), p. 18: "International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed."
- Island of Palmas case (Netherlands, USA) arbitral award, 4 April 1928, VOLUME II pp. 829-871, p. 838: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. The development of the national organisation of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations."

UN GGE report 2015 A/70/174, 'Chapter VI: How international law applies to the use of ICTs'

- Para. 26: "In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality, settlement of disputes by peaceful means (...)refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any state (...) and non-intervention in the internal affairs of other States."
- Para. 27: "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."

Norm

> States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

*'Norms', para. **13(i)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

This norm relates as well to the **due diligence principle** (see **norm c**).

Norm

> States should encourage reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

*'Norms', para. **13(j)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

This norm relates to the **due diligence principle** as well as the **prevention of threats to international peace and security**.

> For the due diligence principle see **norm c**.

> Art. 1: The purpose of the United Nations are:

1) To maintain international peace and security, and to that end: to take effective collective measures for the **prevention and removal of threats to the peace**, and for the **suppression of acts of aggression or other breaches of the peace**, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace".

Norm

> States should not conduct or knowingly support activity to harm the information systems of the unauthorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incidents response teams) of another state. A state should not use authorized emergency response teams to engage in malicious international activity.

*'Norms', para. **13(k)**, UNGGE Report 2015, UN Doc. A/70/174*

International Law

The norm relates to the due diligence principle (see **norm c**).

About the author

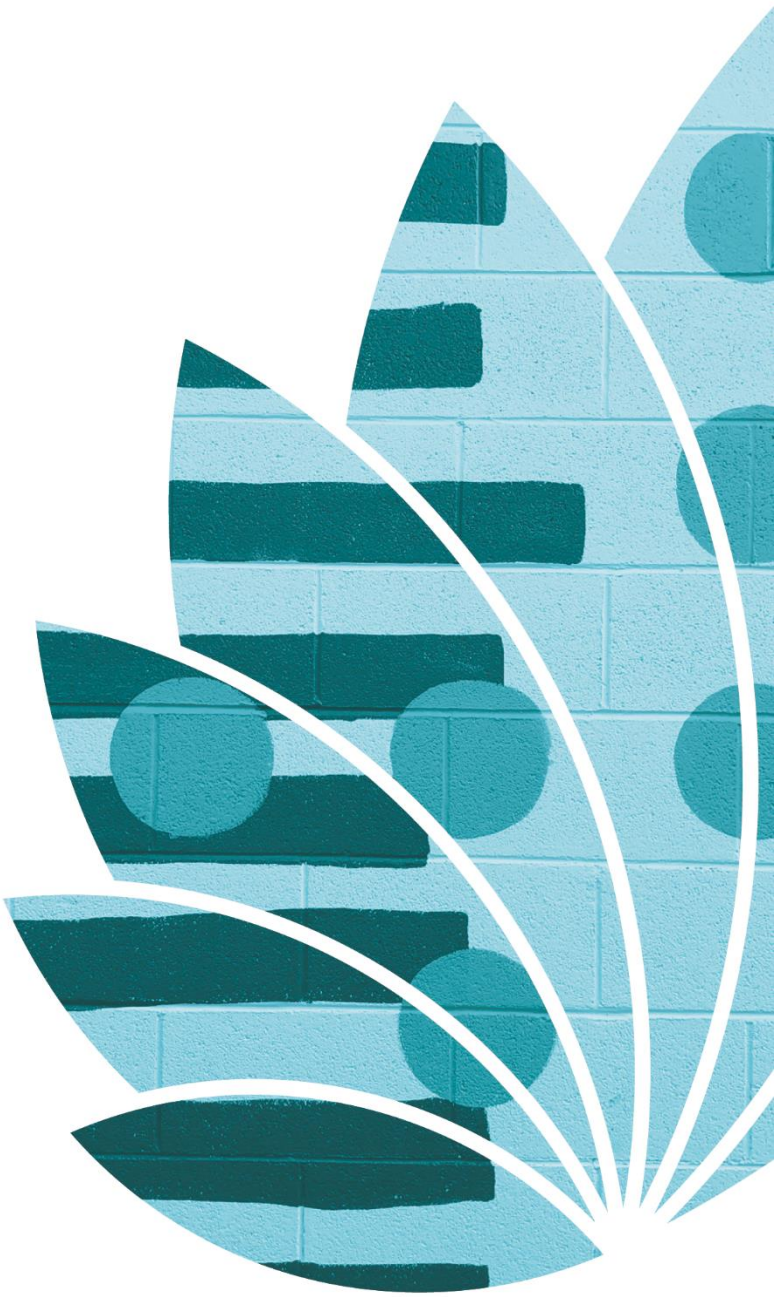
Zine Homburger was a PhD Candidate at Leiden University within the The Hague Program for Cyber Norms. Zine has an educational background in International Relations (BA), Public International Law (LLM) and European Law (LLM) in Germany and The Netherlands. Previously, Zine researched topics related to international environmental law and climate policy as well as human rights and security policies. Her research at the Leiden University focused on the debate on international norms for state behaviour in cyberspace placed at the intersection of international law and international relations. Specifically, she examined the development of the 'do no-harm' norm which encompasses the application of the due diligence principle, the definition of harm among different states and the discussion on the establishment of responsibility or liability and respective responses. Her research interest lie at the intersection of international law, international relations and cybersecurity governance.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.



EU CYBER DIRECT

This project is funded by the European Union.