Revista Española de Derecho Internacional
Sección FORO
Vol. 69/2, julio-diciembre 2017, Madrid, pp. 281-289
http://dx.doi.org/10.17103/redi.69.2.2017.2.01

ISSN: 0034-9380; E-ISSN: 2387-1253

II. FORO

Coordinación a cargo de
Luis HINOJOSA, Manuel DESANTES
y José Luis DE CASTRO

ENSURING CYBERSECURITY THROUGH INTERNATIONAL LAW

Matthias C. KETTEMANN*

1. INTRODUCTION

1. Be in online or offline, be it in the kinetic world or in cyberspace: we need norms —and have always needed them—. «In the long march of mankind from the cave to the computer», as Malcolm N. Shaw puts it in his introduction to international law, «a central role has always been played by the idea of law —that order is necessary and chaos inimical to a just and stable existence—» [1].

2. This contribution examines the protection of cybersecurity under international law and develops a future-oriented approach to increasing cybersecurity through international law [2]. After outlining my concept of cybersecurity and explaining why protecting cybersecurity lies in the common interest of all states (2), I will outline which international legal norms protect cybersecurity (3). The conclusions (4) include perspectives on how to better protect cybersecurity in international law.

* Post-doc fellow at the Cluster of Excellence «The Formation of Normative Orders», University Frankfurt am Main, and co-chair of its Research Focus «Internet and Society» (*matthias.kettemann@normativeorders.net*). All referenced web pages were last consulted on May 31, 2017.

[1] SHAW, M. N., *International Law*, Oxford, 6th ed., Oxford University Press, 2008, p. 1.

[2] The contribution draws on a study conducted by the author for the Deutsche Telekom.

2. TOWARDS A COMPREHENSIVE CONCEPT OF CYBERSECURITY

2.1. Cybersecurity: between security and freedom

3. Cybersecurity is defined very broadly by some states, and covers risks and threats such as cyberwarfare, cyberterrorism, cybercrime and cyberespionage[3]. There is no doubt that cybersecurity is crucial part of national domestic, security, foreign and defense policy[4]. As a central theme of Internet policy[5], cybersecurity is closely linked with the stability, robustness, resilience and functionality of the Internet[6]. Cybersecurity can be threatened by cybercrime and cyberterrorism, but also by a lack of legal and technical cooperation between states and a lack of preventive measures, such as developing crisis intervention centers and teams, as well as transnational crisis communication structures for cyber incidents.

4. The May 2017 WannaCry Ransomware attack, for example, shows how vulnerabilities are caused by a number of factors, including software companies who fail to provide updates or no longer service vulnerabilities, affected companies that have slow patch cycles, secret services that stockpile vulnerabilities, and states that do not force essential service providers (like healthcare companies) to ensure that their systems are stable and secure[7].

5. Fostering and ensuring cybersecurity are a prerequisite for the stability of national economic processes and the international business and financial system, for transnational communication flows, and for the functioning of energy grids, the enforcement of human rights, and the performance of national, regional and international defense infrastructures. Ultimately, cybersecurity is fundamental to the full realization of all human rights.

6. It is too often the case that (cyber) security is contrasted with (Internet) freedom. This view misses the point. As emphasized in the Cybersecurity Strategy for Germany from 2016, what matters is that ensuring both freedom *and* security are among the core duties of the state —offline and online—: «It is therefore the duty of the state vis-à-vis the citizens and enterprises in Germany to protect them against threats from cyberspace and to prevent and

---

[3] Ebert, H. and Maurer, T., «Cybersecurity», *Oxford Bibliographies*, January 11, 2017, available at *http://oxfordbibliographiesonline.com/view/document/obo-9780199743292/obo-9780199743292-0196.xml*.

[4] Most states have Cybersecurity Strategies. For an overview,see NATO Cooperative Cyber Defense Centre of Excellence, Cyber Security Publication Library, available at *https://ccdcoe.org/publication-library.html*.

[5] Segal, A., *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age,* New York, Public Affairs, 2016.

[6] Tikk-Ringas, E. (ed.), *Evolution of the Cyber Domain: The Implications for National and Global Security*, London, Routledge, 2015.

[7] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *WannaCry Campaign: Potential State Involvement Could Have Serious Consequences*, 16 May 2017, available at *https://ccdcoe.org/wannacry-campaign-potential-state-involvement-could-have-serious-consequences.html*.

pursue crime in cyberspace»[8]. Similarly, the Spanish National Cybersecurity Strategy of 2013 is aimed at ensuring that Spain «makes practical use of ICT systems, reinforcing the capacities of prevention, defence, detection and response to cyber-attacks, and building confidence in the use of ICTs»[9].

7. National documents define cybersecurity differently. The Cybersecurity Strategy for Germany defines cybersecurity as «IT security of the networked or network-capable information technology systems at the data level in cyberspace»[10]. This definition is very technology-oriented and too shortsighted in light of how cybersecurity is practically perceived by business and society. The security in the Internet and of the Internet cannot be simply equated with the security of systems and data. Each meaningful cybersecurity concept should be comprehensive and value-based: a commitment to a stable, secure, resilient, fully functional, open and free Internet and its protection against state and private attacks of any kind[11]. The state can only live up to its duties under the requirements of the information society if it offers all stakeholders «protection and freedom of development, and thereby sufficiently secures its own systems» in cyberspace too[12]. This applies to each and every state. Consequently, all states have an interest in increasing cybersecurity.

2.2. Cybersecurity lies in the common interest of all states

8. Even if the definitions of cybersecurity may differ greatly, cybersecurity is a common interest of all states. This community interest is not an aggregate of the individual sets of interests; rather, it lies at their intersection. If a protected interest is part of the community interest, this entails consequences relevant to international law. States are therefore responsible to the international community with regard to cybersecurity according to their judicial authority over critical infrastructures pertinent to it[13].

9. As early as in 2013 the *UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (GGE) determined that the application of norms de-

---

[8] German Federal Ministry of the Interior, Cyber-Sicherheitsstrategie fur Deutschland 2016 (Cybersecurity strategy for Germany 2016), available at *https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf*, para. 8.

[9] Gobierno de España-Presidencia del Gobierno, Estrategia de Ciberseguridad Nacional, 2013, p. 4, available at *http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf*. Cf. Cendoya, A., «National Cyber Security Organisation: Spain,» Tallinn, 2016, pp. 1-22, p. 9, available at *https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SPAIN_092016.pdf*.

[10] Cyber-Sicherheitsstrategie für Deutschland 2016, *cit*., note 8, p. 24.

[11] Cf. Schaake, M. and Vermeulen, M., «Towards a values-based European foreign policy to cybersecurity», *Journal of Cyber Policy*, vol. 1, 2016, Issue 1, pp. 75-84.

[12] Cyber-Sicherheitsstrategie für Deutschland 2016, *cit*., note 8, p. 8.

[13] For documentation of the reports of individual member states, see the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: *http://www.un.org/disarmament/topics/informationsecurity*.

rived from existing international law is «essential» to minimize risks to world peace and international security and stability[14]. Viewed in the context of information technology challenges, cybersecurity is now one aspect of «world peace»[15]. The group went even further in its 2015 report[16], stating inter alia that the international community aspires to regulate the Internet in a peaceful manner «for the common good of mankind».

3. CYBERSECURITY IN INTERNATIONAL LAW

3.1. International law and the Internet

10. International law is the only area of law with which global (public) goods can be managed and global public interest protected[17]. The ubiquity of the technology underlying the Internet, which is not restricted by national borders, renders strictly *single-state* regulation largely ineffective. International law is needed to legitimately and effectively ensure cybersecurity in the common interest of all states. This is not a new insight[18]. Without legitimate and effective protection of cybersecurity under international law, individuals and societies cannot develop to their full potential.

3.2. Cybersecurity in international treaty law

11. International law applies to the Internet[19]. Individual norms from the Charter of the United Nations (UN) (*e. g.* the ban on aggression and intervention) are relevant to the international law of cybersecurity[20]. However,

---

[14] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, June 24, 2013, para. 16 [hereinafter: «GGE report (2013)»].

[15] *Ibid*.

[16] Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary General, A/70/174, July 22, 2015, available at *https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf* [hereinafter: «GGE report (2015)»].

[17] Detailed comparisons: Kettemann, M. C., *Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht,* Bonn, Friedrich-Ebert-Stiftung, 2015. Available at *http://library.fes.de/pdf-files/akademie/12068.pdf*.

[18] UN General Assembly Resolution 53/70, Developments in the field of information and telecommunications in the context of international security, A/RES/53/70, of January 4, 1999, para. 2 lit. c., available at *http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70*.

[19] The scope of this study does not allow for going into detail on all applicable principles of international law. See instead: Schmitt, M. N. and Vihul, L., «The Nature of International Law Cyber Norms», *Tallinn Paper*, No. 5, 2014 (NATO CCD COE), pp. 1-31, p. 16, *https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf*; and Ziolkowski, K., «General Principles of International Law as Applicable in Cyberspace», in Ziolkowski, K. (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publications, 2013, pp. 135-184, pp. 151-152.

[20] See 3.3. below. The ban on aggression and intervention is based on international treaty law, but also on customary international law.

there is no single treaty that is primarily concerned with regulation of the Internet and the key topic of cybersecurity. Although treaties provide (legal) certainty (especially in the eyes of powerful states or states relying on traditional sovereignty concepts)[21], bilateral cybersecurity treaties usually do not live up to the complexity of the issue due to the universality of the Internet, while multilateral treaties can only be attained through lengthy negotiation processes with an uncertain outcome[22]. There is still no treaty on cybersecurity, though. Binding international law on cybersecurity can therefore only be derived to date from customary international law and the principles of international law.

3.3. Cybersecurity and customary international law

12. In the Tunis Agenda adopted at the UN World Summit on the Information Society (WSIS) and in the Tunis Commitment (2005), states committed themselves to a «people-centred, inclusive and development-oriented Information Society, premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights»[23], to «the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration»[24]; to a stable and secure Internet as a worldwide institution, and to the multi-stakeholder approach[25]. Of particular importance for protecting cybersecurity by means of international law is the commitment to international law and the significance of the Internet as a —stable and secure— worldwide institution.

13. For one thing, the international body of law pertaining to cybersecurity provides protection based on human rights. Communicators, recipients and the contents of communications are protected by art. 19 of the International Covenant on Civil and Political Rights (ICCPR)[26], parts of which are based on customary law. Along with these state obligations based on individual human rights (prohibiting states to interfere with certain communica-

---

[21] «USA und China wollen Vertrag zur Begrenzung von Cyberangriffen», *Heise.de,* September 20, 2015, *https://www.heise.de/security/meldung/USA-und-China-wollen-Vertrag-zur-Begrenzung-von-Cyberangriffen-2822083.html.*

[22] Cf. Goldsmith, J., «Cybersecurity Treaties. A Skeptical View», *Hoover Institution Future Challenges Essays*, 2011, pp. 1-16. Available at *http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf*; and Litwak, R. S. and King, M., «Arms Control in Cyberspace?», *Wilson Briefs*, Wilson Center Digital Futures Project, 2015, pp. 1-7, available at *https://www.wilsoncenter.org/publication/arms-control-cyberspace*.

[23] World Summit on the Information Society, Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, November 18, 2005, No. 2, available at *http://www.itu.int/net/wsis/docs2/tunis/off/7.html*.

[24] *Ibid*., No. 3.

[25] WSIS, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6 (Rev.1)-G, November 18, 2005, No. 31, available at *http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.*

[26] International Covenant on Civil and Political Rights, available at *http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.*

tive rights), positive obligations related to Internet infrastructure can also be derived from the state obligations to provide protection and assurance pertaining to information- and communication-related rights.

14. Particularly relevant to ensuring and promoting cybersecurity are the following principles of international law[27], some of which have been translated into treaty law in the UN Charter, are protected under customary international law or are recognized as part of the general principles of international law: sovereign equality, the ban on aggression and intervention, peaceful settlement of disputes, the protection of human rights, the cooperation principle (which draws on the principle of good neighborliness («no harm») and the precautionary principle («due diligence»).

15. The principle of sovereign equality [art. 2 (1) of the UN Charter] is a key principle of international law[28]. Each state has jurisdiction and power over its territory and over the ICT infrastructure located there; this also means, however, that it bears a responsibility to ensure that no attacks against other states or institutions, which would infringe on international law, are organized or carried out from its territory.

16. In addition, the non-intervention principle (art. 2 (7) UN Charter) can be brought to fruition: an intense damage to Internet functionality in another state (e.g. by cyber attacks) could constitute an intervention, although attribution problems will regularly arise[29]. Only some of the attacks originating from the territory of a state represent an «intervention» in terms of international law, because most attacks will be attributable to non-governmental protagonists or to protagonists whose association with governmental agencies cannot be proven.

17. The ban on aggression [art. 2 (4) of the UN Charter] prohibits states from using measures of power beyond simple «intervention» (the former being stated in the non-intervention principle). In the context of the Internet, this article could only be applied to especially serious cases of cyber-attacks with substantial kinetic effects.

18. The principle of good neighborliness (art. 74 of the UN Charter), or «no harm» principle, can be considered as a global principle in the Internet era. Originally only relevant in terms of the relationship with adjacent states, the principle has been gradually extended[30]. In the *Corfu Channel* case the ICJ described the principle as «every state's obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states»[31].

---

[27] GGE report (2015), *cit.*, note 16, para. 26.

[28] Besson, S., «Sovereignty», in Wolfrum, R. (ed.), *Max Planck Encyclopedia of Public International Law (MPEPIL)*, (2008) (2011), para. 1.

[29] Schulze, S.-H., *Cyber-«War», Testfall der Staatenverantwortlichkeit*, Tübingen, Mohr, 2015.

[30] Cf. UN General Assembly Resolution 46/62, Developing and strengthening of good-neighbourliness between States, A/RES/46/62 of December 9, 1991, para. 2 (Good neighborliness is an obligation, «whether or not they [the states] are contiguous»).

[31] *Corfu Channel Case (UK v. Albania)*, ICJ Reports 1949, p. 22.

The «no harm» principle has its roots in the *Trail Smelter*[32] and *Lac Lanoux*[33] cases and has crystallized, through normative vectors such as Principle 21 of the Stockholm Declaration (1972)[34] and Principle 2 of the Rio Declaration (1992)[35], into customary law.

19. In the preventive dimension of the «no harm» principle, a state must take measures to prevent such hazards. Among other things, a commitment to an appropriate infrastructure, the development of emergency plans and the establishment of an international crisis cooperation structure (and culture) can be construed from this.

20. The precautionary principle («due diligence») is of special importance for cybersecurity. Firstly, the «due diligence» principle entails information and consultation obligations[36]. In the scientific world, it is controversial as to what extent the precautionary principle has a «due diligence» dimension or whether the precautionary obligations of states are covered in practice by the «no harm» principle. The principle of «due diligence» was also applied in the field of combating terrorism and the financing of terrorism[37].

3.4. In particular: preventive customary obligations

21. With some justification, normative principles for the regulation of cybersecurity can therefore be derived from the principle of «due diligence». As a result, it is the responsibility of states, inter alia ensuing from this principle, to prevent cyber-attacks originating from their own territory and to (proactively) establish a legal system that ensures and fosters cybersecurity[38]. This can be fulfilled, for instance, by «passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states of cyberattacks that originated from within their borders»[39].

22. In its preventive dimension, the «due diligence» principle helps to identify the obligations of states with regard to cybersecurity, particularly

---

[32] *Trail Smelter Case (United States v. Canada),* First decision, (1949) III RIAA 1905, (1941) 35 AJIL 684, April 16, 1938, Arbitration.

[33] *Lake Lanoux Arbitration (France v. Spain),* (1963) XII RIAA 281, (1961) 24 ILR 101, November 16, 1957, Arbitration.

[34] Stockholm Declaration of the United Nations Conference on the Human Environment, UN Doc A/CONF.48/14/Rev.1, 3, UN Doc A/CONF.48/PC/6, Principle 21.

[35] Rio Declaration on Environment and Development [United Nations Environment Programme (UNEP)] UN Doc A/CONF.151/5/Rev.1, UN Doc A/CONF.151/26/Rev.1 Vol.1, Annex 1, Principle 2.

[36] Koivurova, T., «Due Diligence», in Wolfrum, R. (ed.), *op. cit*., note 28, para. 3.

[37] Cf. Proulx, V.-J., «Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?», *Berkeley Journal of International Law*, vol. 23, 2005, Issue 3, pp. 615-668, p. 629.

[38] Schmitt, M. N., «In Defense of Due Diligence in Cyberspace», *Yale Law Journal Forum,* vol. 125, 2015, pp. 68-81.

[39] Sklerov, M. J, «Solving the Dilemma of State Responses to Cyberattacks: A Justification for the use of Active Defenses against States Who Neglect Their Duty to Prevent», *Military Law Review*, vol. 201, 2009, pp. 1-85, p. 62.

with regard to cybercrime, global cooperation and establishment of capacities. Cybersecurity due diligence was described as part of customary international law, whereby particularly the following preventive duties have emerged as recognized obligations under international law:

— that governments and other stakeholders bolster cybersecurity and develop cybersecurity strategies to protect crucial infrastructures[40];

— that states (and other relevant stakeholders) work together more closely in the fight against cybercrime and cyberterrorism[41], and that they ratify conventions such as the Convention on Cybercrime of the Council of Europe[42];

— that states conclude treaties promoting cooperation between their police authorities[43];

— that states establish confidence-building measures and increase the level of information sharing, both generally as well as (and especially) in the event of cybersecurity-related incidents[44].

4. CONCLUSIONS

23. In the light of the importance of the Internet for states, business and society, cybersecurity —as a prerequisite for a reliably functioning and secure Internet— has become a global community interest which needs protection. A secure Internet lies in the interest of each individual state and also collectively in the interest of all states of the world as a global community.

24. International law is to be fully applied to the Internet, including with regard to regulating cybersecurity. Customary international law and the general principles of international law particularly restrict (and define) national Internet policy. Each state has protection obligations vis-à-vis the international community —to avert threats to the stability, integrity and functionality of the Internet— which can be derived from customary international law.

25. In addition to post-incident information and communication requirements, preventive obligations arise from the due diligence principle and the tenets of good neighborliness and can in part only be met in cooperation with nongovernmental stakeholders. This binding cooperation principle of customary international law provides mandatory guidance to states in their development of strategies for promoting cybersecurity.

---

[40] Cf. the numerous UN General Assembly resolutions on cybersecurity, including UN General Assembly Resolution 64/221, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, A/RES/64/211 of March 17, 2010 (with references to further resolutions).

[41] Cf. UN Office of Drugs and Crimes Resolution 22/8, Promoting technical assistance and capacity building to strengthen national measures and international cooperation against cybercrime, UNODC/CCPCJ/2013/RES/22/8, para. 4.

[42] Cf. GGE report (2013), *cit*., note 14, para. 22.

[43] *Ibid*., para. 22.

[44] *Ibid*., para. 26 et seq.

26. The May 2017 WannaCry ransomware attack, for example, shows how vulnerabilities are caused by a number of factors, including companies who fail to provide updates or no longer service vulnerabilities, affected companies that have slow patch cycles, secret services that stockpile vulnerabilities, and states that do not force essential service providers (like healthcare companies) to ensure that their systems are stable and secure.

27. As the NATO Cooperative Cyber Defence Centre of Excellence concluded with regard to the recent WannaCry ransomware attacks, «[c]ampaigns like WannaCry should remind decision-makers of the importance of baseline cyber security, since in this case the victims could have prevented the spread of ransomware by fairly simple security measures»[45]. Be it baseline cybersecurity or more advanced forms that are necessary for states to implement order to meet their obligations under international law: the debate on how best to ensure a stable and resilient Internet for all is far from over —and it is international law that provides the impetus, frame and objective of the debate—.

28. Any attempt to embrace cybersecurity in international law must be preceded by the recognition of the significance of the multistakeholder approach in the normative development of international Internet law[46]. Yet multistakeholder forums are very ill-suited to drafting binding international law. The most promising approach for embracing binding cybersecurity norms in the long term is the negotiation and adoption of an international treaty. Treaties remain the «gold standard» of international law. The United Nations Framework Convention on Climate Change[47], which entered into force on November 4, 2016, has shown that even today international treaties covering complex topics such as regulations relating to important global public goods can be successfully concluded. There can be no doubt that cybersecurity as a prerequisite for a well-functioning Internet is worth the normative effort.

Palabras clave: Derecho de Internet, ciberseguridad, diligencia debida, vecindad, interés común, enfoque multisectorial.

Keywords: Internet law, cybersecurity, due diligence, neighbourliness, common interest, multistakeholder approach.

[45] CCDCOE, *WannaCry Campaign: Potential State Involvement Could Have Serious Consequences*, *cit*., note 7.

[46] See KETTEMANN, M. C., «Grotius goes Google: Der Einfluss der Internet Governance auf das Völkergewohnheitsrecht», in VEDDER, Ch. (ed.), *Tagungsband 37. Österreichischer Völkerrechtstag 2012*, Vienna, 2013, pp. 89-104.

[47] United Nations Framework Convention on Climate Change, available at *http://unfccc.int/2860.php*.