International Law in Cyberspace: Leveraging NATO's Multilateralism, Adaptation, and Commitment to Cooperative Security

Steven Hill and Nadia Marsan

Cite as: Hill, Steven, and Nadia Marsan. 2020. "International Law in Cyberspace: Leveraging NATO's Multilateralism, Adaptation, and Commitment to Cooperative Security." In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg, 173-185. London: Rowman & Littlefield International.

More information about the book and The Hague Program for Cyber Norms is available on:

www.thehaguecybernorms.nl

Chapter 8

International Law in Cyberspace

Leveraging NATO's Multilateralism, Adaptation, and Commitment to Cooperative Security

Steven Hill and Nadia Marsan[1]

Cybersecurity has become a key component of national security calling for effective international cooperation. As the NATO Secretary-General highlighted, "today, a cyber-attack can be as destructive as a conventional attack, and practically every conflict has a cyber dimension. So being able to defend ourselves in cyber space, is just as important as defending ourselves on land, at sea and in the air."[2] A credible international legal framework is a necessary enabler to a peaceful, secure, and stable cyberspace. The application of international law to cyberspace is now broadly accepted.[3] However, the lack of clarity as to how international law applies has fueled debates on the application of important areas of international law to cyberspace, such as the law of state responsibility, the law of self-defense, and international humanitarian law. Toward maintaining peace and security in cyberspace in line with Article 1 of the Charter of the United Nations[4] and Article 3 of the North Atlantic Treaty,[5] there is value in gaining greater clarity on what constitutes acceptable peacetime behavior in cyberspace and what actions could call for legally justified responses.

Within this context, normative constraints can contribute to preventing conflict in cyberspace by promoting stability and the rule of law and by facilitating transparency and confidence building between states. States set the parameters which form the basis of norms for responsible state behavior according to their consistent practice and expressed intentions. States have at times been reluctant to establish potentially binding rules when the underlying technology and the corresponding threats to cybersecurity are evolving in such a dynamic way. Nevertheless, there has generally been broad consensus

and support for the development of voluntary cyber norms themselves in order to set some parameters and build trust between states in cyberspace in the context of the United Nations.[6] These efforts continue to be underway at this time of publication. Despite such support for the establishment of voluntary norms in cyberspace, reaching agreement on the substance of those norms has proven to be difficult at times.[7] Without prejudice to ongoing discussions at the United Nations and other fora, NATO, bringing together twenty-nine sovereign nations for collective defense within the legal framework of the North Atlantic Treaty,[8] can potentially add value to this debate. The organization provides a forum for daily multilateral discussions and exchanges of views on collective security issues, including cyber defense. Multilateralism as practiced at NATO is a process of continuous consultation based on shared values in the spirit of cooperation.[9] NATO also provides a venue where member states can express support or alignment with a position or with principles expressed by individual allies. The regular meetings of heads of state and government provide an opportunity for member states to make clear public statements on common security priorities. Since 2008, cyber defense has featured prominently in all summit declarations. For example, at the Warsaw Summit in 2016, allies affirmed that cyberattacks present a clear challenge to the security of the alliance and could be as harmful to modern societies as a conventional attack.[10] At the Wales Summit in 2014, NATO heads of state and government underlined that NATO's cyber policy must reaffirm, "the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defense."[11]

NATO is not a state but an international organization. As such, NATO does not create international law or voluntary norms that regulate state behavior. There would be little appetite among allies and in the broader international community for NATO to lead the global debate on the development of voluntary norms for responsible state behavior in cyberspace. That said, as a multinational intergovernmental organization, NATO provides a good vantage point from which to observe and note emerging state practice. The organization has followed with interest the debates in various international fora on how to make cyberspace safer and more secure since such efforts actually set important parameters and frame policy discussions on collective defence. At the Brussels Summit in July 2018, allies affirmed NATO support for "work to maintain international peace and security in cyberspace and to promote stability and reduce the risk of conflict, recognizing that we all stand to benefit from a norms-based, predictable, and secure cyberspace."[12]

Written from the perspective of two practitioners, this chapter will begin by expanding on the role of norms in the promotion of international peace and security, and will then propose four areas within NATO's mandate where allies could potentially contribute to the socialization of broad voluntary

norms. The chapter concludes that although states are responsible for norms, given the proliferation of cyber threats to transatlantic security, NATO cannot but both contribute to and draw guidance from the ongoing debates on the development of norms of responsible state behavior and stability in cyberspace. Furthermore, recent experience in NATO and in other international fora has underlined the importance of reinforcing effective enforcement mechanisms and potential response options.

NORMATIVE CONSTRAINTS AND CYBERSECURITY

NATO heads of state and government affirmed at the Wales Summit in 2014 that international law, including international humanitarian law and the UN Charter, applies in cyberspace.[13] Although there is now general consensus on the fundamental role that international law can play in promoting peace and stability in cyberspace, questions remain as to how international law applies in a cyber context. For example, questions relating to attribution and state responsibility, which have always been difficult topics in international law, have become even more so given the intrinsically anonymous and asymmetrical nature of cyberspace. There are also questions as to whether a particular cyber activity is of such a nature to warrant a response, preventative or defensive. The "below-the-threshold" nature of most malign cyber incidents challenges our understanding of what counts as an internationally wrongful act which could form the basis of a legally justified response such as countermeasures. The lack of clarity in these crucial and contentious areas makes it difficult to predict state action in the cyber realm and the existence of divergent views among states risks leading to misperceptions and potential escalations.[14]

Several important international initiatives have provided some guidance on these and other questions. The development of the two *Tallinn Manuals* under the auspices of the NATO-accredited Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Estonia has helped identify the key legal issues and provides an academic assessment of the application of international law to cyberspace. As the development of the manuals was not a process formally endorsed by states, experts were free to thoroughly explore the implications of legal issues and states had an opportunity to offer comments during the so-called Hague Process. The manuals have become indispensable desk books for lawyers and cyber policy experts. However, although the *Manuals* help us interpret the law, they are not official NATO doctrine and do not constitute the law itself.

There has been progress in advancing the norms debate in international fora, many of which have largely been aspirational in nature.[15] The United Nations

Group of Government Experts, a United Nations working group of experts from member states, was created to study "potential threats in the sphere of information security." The 2016/2017 Group was to consider measures to address these threats, including "norms, rules, and principles of responsible behavior of states, confidence building measures, and capacity building."[16] The Group's failure to arrive at a consensus report and robust substantive rules highlighted, for some, the reluctance of states to seriously engage on the question of the application of international law in cyberspace. These efforts continue at the time of publication under the auspices of two bodies: a Group of Governmental Experts and an Open-Ended Working Group.

National initiatives such as the London and the Hague Processes as well as recent statements made by NATO allies have contributed to further clarifying some elements of contention on the application of international law to cyberspace. A former legal adviser at the US Department of State, Harold Koh, set out early in the process that international law applies to cyberspace and that the development of common understandings about how these rules apply will promote greater stability in cyberspace.[17] In 2017, another former legal adviser at the US Department of State, Brian Egan, confirmed that from the US perspective, the international law of state responsibility supplies the needed standards for attributing acts, including cyber acts to states.[18] More recently, the former UK attorney general Jeremy Wright elucidated the UK interpretation of several key components of international law as they apply in cyberspace, including on the application of the UN Charter, the unlawful intervention on state sovereignty and the corresponding use of countermeasures.[19] Commemorating one year of the *Tallinn Manual 2.0*, the Minister of Foreign Affairs of the Netherlands, HE Mr. Stef Blok, affirmed the Dutch position that there is no need to develop a new system of international law for cyberspace, arguing that the clear application of existing laws in cyberspace is the best guarantee of an open, free, and stable Internet in the future.[20]

These important statements and international efforts have all contributed to setting some important parameters for the debate. Indeed, clear national statements about the applicable legal framework enhance cyber stability by increasing predictability. States, especially those with advanced cyber capabilities, should be "open and clear in setting out the rules" they feel bound by since, in doing so, they "demonstrate not just [their] commitment to the rules based international order, but also [their] leadership in its development."[21] States themselves set out the normative constraints that bind them in their international relations; domestic sources of "law are found in statutes and in court judgments—but there are few of either in international law, instead there are treaties, and customary international law formed from the general and consistent practice of states acting out of a sense of obligation."[22]

Cyber defense is part of NATO's core task of collective defense, within NATO's broader deterrence and defense posture which was strengthened at

the NATO Summit in Wales in 2014. Mechanisms used in deterrence, including denial by defense and the development of voluntary norms, are intended to dissuade or diminish the likelihood of unacceptable behavior by making the costs of the bad actions exceed the benefits to be gained therefrom.[23] A "norm" is broadly understood as "a collective expectation of proper behavior of actors with a given identity."[24] Although norms are not legally binding in themselves, "laws can serve as a basis for formulating norms, just as norms can be codified by law."[25] In distinguishing between formal international law and voluntary nonbinding norms, Brian Egan notes that norms "set out standards of expected state behavior that may, in certain circumstances, overlap with standards of behavior that are required as a matter of international law. Such norms are intended to supplement existing international law. They are designed to address certain cyber activities by States that occur outside the context of armed conflict that are potentially destabilizing."[26]

Within NATO's legal framework of the North Atlantic Treaty, the utility of norms is not so much geared toward inducing a negative impact on detractors' reputation or soft power, but rather toward elucidating how allies apply and interpret their commitments under the North Atlantic Treaty in cyberspace, thereby increasing predictability and clarifying where collective NATO action may be legally justified.

As described above, NATO can provide an important forum for member nations to discuss cyber defense. The foundational elements of NATO's approach to cyber defense include a respect for and inviolability of the sovereign nature of allies' cyber defense capabilities, strong political oversight by allies, and the requirement for consistency with NATO obligations and international law. These commitments provide a reassuring environment where allies show mutual respect of each other's sovereignty and need for political oversight, while encouraging constant dialogue, cooperation, and assurance that threats to cybersecurity will be addressed in line with international law.

In their chapter "International Norm Dynamics and Political Change," Martha Finnemore and Kathryn Sikkink develop the idea of a three-stage "norm life cycle" from norm emergence to norm acceptance to internalization. Between the first and second stages, they identify a "tipping point" whereby a critical mass of relevant state actors adopt the norm.[27] The second stage also called "norm cascades" is animated by states and international organizations toward increasing legitimacy through institutionalization.[28] NATO could act as a socialization venue precisely at the tipping point between norm emergence and norm acceptance. Indeed, the multilateralism of the alliance can function as an agent of socialization by encouraging states within the alliance, by virtue of their identity as members of a group tied by shared values, to adopt common policies and to subscribe to the set standards of expected state behavior in cyberspace.[29] If we look at the timeline of UNGGE decisions[30] and NATO heads of state and government decisions on cyber since 2012,

we see that NATO provided an opportunity for a group of nations united by shared values to socialize and affirm principles that emerged in other international fora, the UN GGE in this case. This should not be underestimated as what may begin as a general, shared and nonbinding principle can, by virtue of state practice and a sense of legal obligation, "crystallize into binding customary international law" over time.[31]

NORMS, DETERRENCE, AND NATO

Within NATO, allies have coalesced on a few fundamental areas that can serve as building blocks for the development and particularly the socialization of norms: the rule of law, restraint, resilience, and mutual cooperation and assistance. These areas are well anchored in the North Atlantic Treaty and in the most recent Summit Communiques, which supplement the work of international expert groups regarding how well-established areas of international law apply to cyberspace.

Rule of Law

Allies express their commitment to the rule of law in the preamble to the North Atlantic Treaty which states that "the Parties to this Treaty . . . are determined to safeguard the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law." At the NATO Summit in Wales in 2014, allies recognized that "international law, including international humanitarian law and the UN Charter, applies in cyberspace."[32] More recently, at the Brussels Summit in July 2018, allies reaffirmed their "commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable."[33]

The broad affirmation of the application of the body of international law to cyberspace cannot be underestimated. It is the essential starting point toward ensuring predictability and stability as it places a duty on states to exercise diligence in the application of international law in cyberspace. At the NATO Summit in Warsaw in 2016, NATO heads of state and government recognized cyberspace as an operational domain "in which NATO must defend itself as effectively as it does in the air, on land, and at sea."[34] Together with the commitment to respect the UN Charter and international humanitarian law, the designation of cyberspace as an operational domain indirectly reinforces the tenet that the general corpus of international law applying in the air, land, and sea domains also applies in cyberspace. Although every situation is unique and states must be able to respond to cyber incidents using a

wide variety of means, states have the obligation to act in accordance with international law before (*jus ad bellum*) and during an armed conflict (*jus in bello*) as well as during peacetime.

With the application of international law in cyberspace, it can be inferred that there is no immediate requirement to create new legal instruments to govern state behavior in cyberspace. Such proposals, including the idea of a Digital Geneva Convention[35] or of an International Code of Conduct for Information Security,[36] have raised a number of concerns on the part of some states related to enforcement, verification, volatile technological change, and fear that tailored instruments may discredit rather than reinforce the international legal order.[37] With respect to the proposal for an International Code of Conduct for Information Security, the primary concern was that such a code could potentially enshrine state sovereignty and information control in cyberspace.[38]

Restraint

Flowing from the previous point on the rule of law, NATO discussions and statements also support an evolving consensus on the application of the principle of restraint in cyberspace. Article 1 of the North Atlantic Treaty embodies the principle of restraint which echoes the principles set out in Article 1 of the UN Charter: "the Parties undertake, as set forth in the Charter of the United Nations, to settle any international dispute in which they may be involved by peaceful means in such a manner that international peace and security and justice are not endangered, and to refrain in their international relations from the threat or use of force in any manner inconsistent with the purposes of the United Nations."[39]

At the Warsaw Summit in 2016, allies agreed that they "will continue to follow the principle of restraint and support maintaining international peace, security and stability in cyber space."[40] States have shown that they generally respond to cyber incidents at a lesser threshold than would be permitted under international law, thereby demonstrating a commitment to restraint and de-escalation. Some good examples of such responses include network shutdown to stop the spread of a particular attack, public attribution, diplomatic demarches, economic sanctions, and increased exchanges of information with like-minded states. Self-restraint in cyberspace is especially important as actions in that realm may have unintended and serious follow-on consequences for other state and non-state actors: "the very newness of cyberwar and the fear of unforeseen consequences in unpredictable systems may contribute to prudence and self-restraint that could develop into a norm of non-use or limited use or limited targets."[41] The importance of self-restraint in cyberspace is further highlighted within the context of "broad deterrence,"

which includes the notion of entanglement. Entanglement is "the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim."[42]

Resilience

At the Warsaw Summit in 2016, allies adopted the Cyber Defense Pledge toward strengthening and enhancing the cyber defenses of national networks and infrastructures, thereby bolstering the alliance's resilience to cyber threats and enhancing the resilience of the alliance itself. This emphasis on cyber resilience was reaffirmed at the NATO Summit in Brussels in July 2018, where allies declared that they "are determined to deliver strong national cyber defenses through full implementation of the Cyber Defense Pledge, which is central to enhancing cyber resilience and raising the costs of a cyber-attack."[43]

The commitment to resilience is anchored in the North Atlantic Treaty at Article 3: "in order more effectively to achieve the objectives of this Treaty, the Parties . . . will maintain and develop their individual and collective capacity to resist armed attack."[44] Although Article 3 refers to the capacity to resist *armed attack*, NATO's approach to cyber defense through the pledge has prioritized resilience in peacetime, precisely to prevent armed attacks from occurring in the first place. Effective cyber defense and deterrence relies on resilience of networks and their capacity to recover.[45] Resilience of networks deters malicious cyber actors by increasing the effort, raising the risk, and reducing the rewards.[46]

The priority for NATO itself is the protection of the communication and information systems owned and operated by the alliance. In light of our increasing dependence on information technologies and the escalatory potential of state action in cyberspace, the resilience of our cyber networks is necessary to limit the damages of any malicious cyber incidents including cyberattacks and, correspondingly, reinforce collective defense mechanisms themselves. The emphasis on cyber resilience highlights a fundamental element of collective defense; that allies' "interconnectedness means that we are only as strong as our weakest link."[47]

Mutual Assistance and Cooperation

An important enabler to resilience is mutual assistance and cooperation, which is a fundamental principle animating the collective defense engagement of the North Atlantic Treaty.[48] Just as for resilience, Article 3 of the treaty is the anchor for collective assistance: "in order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, *by*

means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."

As part of efforts to enhance information sharing, allies committed to a model memorandum of understanding which sets out arrangements for the exchange of cyber defense-related information and assistance to improve allies' cyber incident prevention, resilience, and response capabilities. In his chapter "The Cyberhouse Rules: Resilience, Deterrence and Defence in Cyberspace," the current assistant secretary-general for Emerging Security Challenges at NATO Headquarters underlined that "cyber defence is a quintessential team sport, and the Alliance recognises that it cannot go it alone in cyberspace: partnerships are instrumental for strengthening resilience and deterrence."[49] This pledge for mutual assistance is a key element toward ensuring the resilience of networks and was reaffirmed at the NATO Summit in Brussels in July 2018.[50]

Although NATO has a regional focus, its commitment to collective security calls for close cooperation with other international organizations, including cooperative relationships with more than forty countries around the world and international organizations. For example, in 2016, a Technical Arrangement on cyber defense was concluded between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU), thereby providing a framework for exchanging information and sharing best practices between emergency response teams. NATO has also recognized the importance of cooperation with the private sector in confronting threats and challenges to cybersecurity, especially as industry develops and operates the vast majority of networks worldwide. Toward increased cooperation with industry, NATO established the NATO-Industry Cyber Partnership at the Summit in Wales in 2014. This was further reaffirmed at the NATO Summit in Brussels in 2018 where allies committed to "further develop our partnership with industry and academia from all Allies to keep pace with technological advances through innovation."[51]

CONCLUSION

There is no need to create specific and tailored law to govern state behavior in cyberspace. It is more a question of applying and adapting existing law to a new and evolving context. Existing multilateral institutions such as NATO, working within the clear international legal framework of the North Atlantic Treaty, could add value in the process of socialization of voluntary norms regulating responsible state behavior in cyberspace, without prejudice to ongoing efforts by states either bilaterally or multilaterally.

To complement these efforts, a multilateral organization such as NATO could be a vehicle for a driver toward identifying common approaches between states. Indeed, multilateral discussions in NATO generally complement and are coordinated with bilateral efforts. As an alliance of sovereign states, NATO has shown that multilateralism and bilateralism can overlap in an effective way. National commitments and positions can be much more effective from a defense and deterrence perspective when supported more broadly by other states. Despite the challenges that broad consultations present, multilateralism will continue to be attractive as a force multiplier and as a foundation for mutual assistance.

It is argued in this chapter that the alliance's role in channeling state positions regarding voluntary norms for responsible state behavior in cyberspace should not be underestimated. NATO's multilateralism can function as a socialization vector by encouraging member states, by virtue of their identity as members of an alliance united by shared values, to adopt policies and national legislation that are animated by their common interests and commitment to a set of fundamental principles including the rule of law, restraint, resilience, and mutual cooperation and assistance. This, in turn, forms a strong basis for the acceptance and eventual internalization of certain voluntary norms for responsible state behavior in cyberspace.[52]

The multilateral nature of discussions at NATO enables another fundamental characteristic of the organization, which is its ability to learn, change, and adapt to emerging security challenges. The former UK attorney general Jeremy Wright recently underlined that "one of the biggest challenges for international law is ensuring it keeps pace as the world changes. International law must remain relevant to the challenges of modern conflicts if it is to be respected, and as a result, play its critical role in ensuring certainty, peace and stability in the international order."[53] NATO's ability to adapt has been one of its greatest strengths over the years. The ever-shifting power dynamics in cybersecurity are what make setting clear rules, consequences, and expectations so difficult. NATO allies, united by shared values and animated by a spirit of continuous adaptation, are well placed to contribute to novel applications of international law within the parameters set out by the North Atlantic Treaty.

Through its broad network of cooperative partnerships, NATO brings together many different actors including nations, international organizations, and industry. As an alliance focused on collective defense, there is a prerogative for greater cooperation in cyber defence, including in information sharing and the building of expert networks, toward establishing a common language, standardized procedures and expertise to ensure the resilience of national and NATO systems. It is by encouraging regular

high-level interaction between national cyber policy experts, lawyers, academics, and industry, that we will gain more clarity on the application of international law.

The application of international law depends heavily on important political factors and will rarely be clarified in a factual vacuum. NATO's regular multilateral cyber defense exercises engage the highest level of government decision makers and are crucial to the development of effective capabilities. These exercises also provide an opportunity to "test" the application of international law and clarify national positions in some particularly contentious areas, albeit in a virtual and usually classified context. Exercises are also a good vehicle for assessing the implementation of practical measures, thereby clarifying the range of actions that can form the basis of acceptable responses to malicious cyber activity.

With cyber defence now being a fundamental facet of North Atlantic security, NATO must continue to be a forum where allies address the collective security implications of cybersecurity. NATO supports the establishment of a norms-based, stable and secure global cyberspace. NATO does not set norms, states do. But with greater cooperation and multilateral dialogue, states could begin to take common national positions regarding the limits of appropriate behavior in well-defined areas. As such, NATO will continue to provide an important forum for multilateral cooperation and engagement in the context of cyber defense, which will in turn support and facilitate debates on how international law should apply especially in collective defense contexts.

NOTES

1. The views expressed here are ours alone and do not necessarily represent the views of NATO or its allies.

2. Stoltenberg, Jens. 2018. "Why Cyber Space Matters as Much to NATO as Land, Sea and Air Defence," *Financial Times*, July 12, 2018. https://www.ft.com/content/9c3ae876-6d90-11e8-8863-a9bb262c5f53.

3. NATO Wales Summit 2014 Communiqué, paragraph 72.

4. United Nations, *Charter of the United Nations*, October 24, 1945, 1 UNTS XVI, hereafter *UN Charter.*

5. *The North Atlantic Treaty 1949.*

6. See the NATO Warsaw Summit 2016 Communiqué, paragraph 70: *We welcome the work on voluntary international norms of responsible state behavior and confidence-building measures regarding cyberspace*.

7. See Nye, Joseph S. 2018. "Normative Restraints on Cyber Conflicts," *Cyber Security: A Peer-Reviewed Journal* 1, no. 4 (August): 331–342. https://www.belfercenter.org/sites/default/files/files/publication/ Nye%20Normative%20Restraints%20Final.pdf.

8. *The North Atlantic Treaty*, Preamble.
9. As reflected in *The North Atlantic Treaty*, Article 9.
10. NATO Warsaw Summit 2016 Communiqué, paragraph 70.
11. NATO Wales Summit 2014 Communiqué, paragraph 72.
12. NATO Brussels Summit 2018 Communiqué, paragraph 20.
13. NATO Wales Summit 2014 Communiqué, paragraph 72.
14. Egan, Brian J. 2017. "International Law and Stability in Cyberspace," *Berkeley Journal of International Law* 35, no. 1, (2017): 169–180, 172. http://scholarship.law.berkeley.edu/bjil/vol35/iss1/5.
15. Including the production of the Cyber Norms Index by the Carnegie Endowment for International Peace, the work of the Global Commission on the Stability of Cyberspace, the London Process and the G20, to name only a few international initiatives.
16. United Nations General Assembly resolution 68/243, *Developments in the field of information and telecommunications in the context of international security*, A/RES/68/243 (December 27, 2013), available from undocs.org/A/RES/68/243.
17. Koh, Harold Hongju. 2012. "International Law in Cyberspace," *Yale Law School Faculty Scholarship Series* 4854 (2012): 1–12. http://digitalcommons.law.yale.edu/lfss_papers/4854.
18. See Egan 2017.
19. Speech delivered by the UK attorney general Jeremy Wright QC MP, *Cyber and International Law in the 21st Century,* May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. Hereafter *Wright.*
20. Blok, Stef. 2018. "Keynote by HE Mr. Stef Blok MA, Minister of Foreign Affairs," *Militair Rechtelijk Tejdschrift* 111, 3 Cyber Special (2018): 8–10. https://puc.overheid.nl/mrt/doc/PUC_248137_11/1/.
21. See Wright.
22. *Ibid.*
23. Nye Jr., Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter): 44–71, 53. doi:10.1162/ISEC_a_00266.
24. Nye 2018, 11 citing Finnemore, Martha and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity," *The American Journal of International Law* 110, no. 3 (July): 425–479, 442. http://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425.
25. *Ibid.*
26. Egan 2017, 180.
27. Finnemore, Martha, and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (Autumn): 887–917, 895.
28. *Ibid.*, 898.
29. *Ibid.*, 902.
30. For example, the UNGGE 2013 affirmed the application of existing international law to states' cyber activities, while NATO did so at its summit in Wales in 2014; the UNGGE 2015 affirmed a state's inherent right to act in self-defense in response to a cyber operation meeting the threshold of an armed attack, while NATO

did so at its Summit in Wales in 2014; UNGGE 2015 confirmed the application of IHL principles to cyberspace, NATO did so at its summit in Wales in 2014.

31. Egan 2017, 180.
32. NATO Wales Summit 2014 Communiqué, paragraph 72.
33. NATO Brussels Summit 2018 Communiqué, paragraph 20.
34. NATO Warsaw Summit 2016 Communiqué, paragraph 70.
35. Proposal initially made by the president of Microsoft Incorporated, Brad Smith, at the RSA Conference in February 2017.
36. Originally presented to the United Nations General Assembly in 2011 by China, Russia, Tajikistan, and Uzbekistan. Subsequently, a revised version was submitted to the United Nations General Assembly in January 2015 by the founding members of the Shanghai Cooperation Organization (SCO).
37. Maurer, Tim, and Kathryn Taylor. 2018. "Outlook on International Cyber Norms: Three Avenues for Future Progress," *Just Security*, March 2, 2018. www.justsecurity.org/53329.
38. *Ibid*.
39. *The North Atlantic Treaty*, Article 1.
40. NATO Warsaw Summit 2016 Communiqué, paragraph 70.
41. Nye 2018, 15.
42. See Keohane, Robert O. and Joseph S. Nye Jr. 1977. *Power and Interdependence: World Politics in Transition.* Boston: Little, Brown.
43. NATO Brussels Summit 2018 Communiqué, paragraph 20.
44. *The North Atlantic Treaty*, Article 3.
45. Nye 2017, 56.
46. *Ibid.*, citing Bruce Schneider, page 56.
47. The NATO Cyber Defense Pledge, issued on July 8, 2016, paragraph 2. https ://www.nato.int/cps/en/natohq/official_ texts_133177.htm
48. *The North Atlantic Treaty*, Preamble: *They are resolved to unite their efforts for collective defense and for the preservation of peace and security*.
49. Missiroli, Antonio. 2018. "The Cyberhouse Rules: Resilience, Deterrence and Defence in Cyberspace," *Italian Institute for International Political Studies*, May 2, 2018. https://www.ispionline.it/sites/default/files/ pubblicazioni/commentary_missiroli_02.05.2018.pdf
50. NATO Brussels Summit 2018 Communiqué, paragraph 20.
51. *Ibid*.
52. See, for example, the NATO Cyber Defence Pledge. https://www.nato.int/cps/en/natohq/official_texts_133177.htm
53. See Wright.

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.