Taming the 'Wild West': The Role of International Norms in Cyberspace

https://www.e-ir.info/2017/11/13/taming-the-wild-west-the-role-of-international-norms-in-cyberspace/

ELIZABETH THOMAS, NOV 13 2017

We live a highly connected world. The increasing ubiquity of the Internet has brought a wide range of social and economic benefits. However, the Internet is also increasingly a source of risk for individuals, businesses, and states. Cyber security is now a core national security interest and cyberspace a new domain of statecraft, posing a range of challenges to international relations. The international system is traditionally defined by the principle of sovereignty – a principle challenged in cyberspace by the lack of territorial borders, and the dominance of the private sector and non-state actors.[1] States are navigating this new domain without a roadmap. While there is some agreement about the application of existing international law to cyberspace, significant questions remain unresolved. As a result, there is a risk that cyber incidents can escalate and threaten international peace and security. Developing norms for state behaviour in cyberspace can help mitigate this risk.

This essay will use emergent cyber-security norms to illustrate the role that international norms play in global security. The essay will proceed in three sections. Firstly, it will outline elements of the social constructivist theory underpinning contemporary discussion of norms, including how norms emerge. Secondly, it will explain the challenges posed by cyber threats to global security and current uncertainties in the application of formal international law. It will argue that in an evolving and highly-complex security environment, norms can reshape global security practices and thereby maintain stability. The final section will use empirical evidence to trace the norm-building processes currently underway, focusing on the discussion of norms for state behaviour in cyberspace under the auspices of the United Nations (UN), and the United States' (US) efforts to create a norm prohibiting cyber-enabled commercial espionage.

A social constructivist approach to norms

The concept of international norms has become commonplace in International Relations scholarship, particularly in neoliberal institutionalist and social constructivist theories.[2] Constructivists agree with neoliberal institutionalists that cooperation is possible in the international system but have a very different account of how that cooperation emerges.[3] Constructivists argue that the world is socially constructed through intersubjective interactions – actors develop understandings of their own and others' identities and interests through norms and practice.[4][5] This essay will focus on a constructivist approach to norms, in which norms constitute as well as regulate state behaviour.

This essay adopts Finnemore and Sikkink's definition of norms as a "standard of behaviour for an actor with a given identity".[6] [7] Interests and identities are not static – they are produced and reproduced through interaction.[8] If a state's interests change, its underpinning identities and norms have shifted.[9] These intersubjective identities also create durable expectations between states, helping to create stability and predictable patterns of behaviour.[10] What distinguishes a norm is a sense of 'ought' – norms prescribe how states should behave.[11] International norms are obeyed by states not because they are enforceable but because they are seen as legitimate.[12] Because norms have a prescriptive force, they also have an evaluative element, and can be invoked both to condemn and condone certain behaviours.[13] In short, norms "create expectations as well as prescribe what appropriate behaviour ought to be."[14]

Norms can have both regulative and constitutive effects on state behaviour. While the latter are internalised and create new interests, regulative effects encourage states to act in accordance with the norm for instrumental reasons.[15] Norms can have regulative effects when states are socialised to behave in accordance with the norm – not because they have accepted its validity, but because of legitimacy or conformity pressures. For instance, naming and shaming can cause a state to alter its behaviour. In changing its behaviour to align with a norm, a state implicitly accepts the value of that norm.[16] The nascent norm prohibiting economic espionage (discussed in the final section of this essay) has arguably had a regulative effect because China probably accepted the norm as a tactical concession.

There are no 'bright-line' rules to indicate when a practice has become a norm, but an argument can be made that norms emerge more quickly in relatively new domains such as cyberspace.[17] Finnemore and Sikkink's three-stage norm "life cycle" model is most often used to explain the emergence of new norms. In this model, the norm life cycle is comprised of three stages: "norm emergence"; a process of socialisation followed by broad acceptance of a norm, termed a "norm cascade"; and finally, norm internalisation.[18] The model illustrates that as norms evolve and cascade, state interests, identities and practices can be significantly altered. In the initial stages, norms are more likely to have only regulative effects – it takes time for states to internalise a norm and for compliance to become habitual.[19] Nevertheless, as norms emerge, we should be able to observe their impact on state behaviour in cyberspace.

Cyberspace: The new "wild, wild West"?

In a globalized world, states are bound closely together in a web of deep economic interdependence, facilitated by Internet connectivity. The Internet is at once the "backbone of the world economy and a significant new venue for attack".[20] Cyberspace is now widely accepted as a fifth domain of warfare, and cyber threats are framed by states as a national security concern.[21] Cyberspace is popularly characterized as an anarchic, lawless domain to the extent that President Obama recently cautioned against it becoming the new "wild, wild West."[22]

In the interest of clarity, this essay does not address the full range of actors in cyberspace (including everything from lone 'hacktivists' to organized crime or terrorist activity), and focuses solely on state-centric cyber threats. Cyber-enabled espionage and offensive cyber capabilities are increasingly commonplace. These tools can harm another state's economic or national security interests. However, the risk of unintended consequences is quite high, given the interconnected nature of Internet systems. Stuxnet, the most destructive cyber threat so far, hit its target but also widely found its way into 'civilian' cyberspace.[23] Further complicating the picture, cyberattacks now are commonplace in peacetime. One estimate suggests that 61 state-on-state cyberattacks have been conducted in peacetime since the late 1980s, along with 24 during wartime.[24]

The diversity, complexity and potential potency of cyber threats poses a risk to international peace and stability. Stability in this context has two elements. First, states have an interest in the stability and security of cyberspace itself, given how critical the Internet has become to both the delivery of basic services and critical national infrastructure. In late 2015, an attack on a Ukrainian power grid left 225,000 people without electricity.[25] Secondly, there is a real risk of kinetic conflict resulting from misunderstandings or misperceptions in cyberspace. This is because there are uncertainties in the application of international law and few shared understandings of what constitutes acceptable state behaviour.

Very few treaties deal directly with cyberspace simply because it is a new domain.[26] Moreover, it is unclear how existing instruments of international law apply in cyberspace. While a group of states agreed in 2013 that international law applies online as it does offline (addressed in more detail in the following section), some states – including China and Russia – have been reluctant to take this view. Significant questions also remain unanswered about *how* international law (including the laws of armed conflict (LOAC) apply in cyberspace.[27]

Key issues include what kind of cyber incident would cross the threshold to constitute an "armed attack" (allowing states to defend themselves with force), and what might constitute a proportionate response to a cyberattack.[28] In 2014, NATO clarified that a cyberattack could possibly trigger NATO's mutual defence guarantee (Article 5) but it

remains unclear how severe an attack would be required.[29] The US stated in 2011 that it would respond to a cyberattack as it would any other threat against the state, but it is not clear where states' red lines are drawn in cyberspace.[30] The 2014 hack of Sony Pictures was not against a government target and did not result in physical damage, but the US government sanctioned a number of North Korean actors and organisations in response.[31]

The Sony hack also highlights that much military and espionage activity is likely to take place over civilian-owned networks, raising complex questions about what constitutes a legitimate target.[32] The 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare* ***[33]*** was an attempt by a group of international legal experts to determine the applicability of the LOAC and international humanitarian law to cyberspace. However, they failed to achieve consensus on many points.[34] Finally, cyberattacks are secretive by their very nature. The nature and consequences of an attack may not be immediately obvious, and the high degree of difficulty in accurately attributing the source of an attack can add to the confusion. In some instances, it is non-state groups aligned to a state government that actually carry out an attack, further confusing issues of attribution.[35]

While Russia (and to a lesser extent China) have pushed for a treaty-based approach to cyber-security, the idea has attracted little support from Western states. Opposition stems from the likely difficulties in developing and implementing a treaty in an area which is still not well understood nor well-defined.[36] Indeed, the emergence of new technologies exemplifies where norms may be required to supplement existing international law and to develop state identities and interests. Many states are reluctant to bind themselves to a treaty in the face of a still-developing technology.[37] Any treaty also would be complicated by the covert, classified nature of cyber capabilities. It would be very difficult to verify and enforce compliance.[38]

These uncertainties and ambiguities increase the odds of misperception and miscalculation, along with the possibility of a cyber action escalating into a kinetic action.[39] Faced with increasing risks to stability and the challenge of developing any kind of workable cyber-security treaty, there has been general agreement that states must begin to develop norms for responsible state behaviour in cyberspace.[40] There is a very broad consensus on the need for norms to build trust and confidence. For instance, in June 2016 Microsoft published a white paper on norms for states and the global information and communications technology (ICT) industry, prompted by concerns that privately-owned infrastructure is often "the battlefield for cyber conflicts and conduit for other attacks launched by governments."[41] Against this backdrop, the role for international norms therefore is to establish standards of behaviour for states operating in a new domain.

Norms, in guiding appropriate state behaviour and reshaping states' interests, can help make cyberspace less 'wild'. States generally have a shared interest an open, secure and stable cyberspace to maximise the economic, social and cultural benefits of the Internet.[42] Developing international norms can help maintain the stability of the Internet and reduce the risk that a cyberattack escalates into broader conflict. In an emerging security area, where the application of international law is unclear, international norms can provide a guide for decision-making and behaviour. Finally, international norms can also provide a foundation for the development of future international law; whether via incorporation into a treaty or because state practice crystallizes into customary international law.[43] Because "[c]yber attack is a behaviour rather than a technology",[44] shaping state behaviour – while difficult – is the only means to improve global security outcomes.

Establishing the 'rules of the road': Emerging cyber security norms

The value of norms also is demonstrated by the emphasis that states have placed on developing norms for cyberspace. A wide range of states have made the development of the 'rules of the road' for cyberspace an explicit foreign policy goal. The fourth Global Conference on Cyberspace was held in April 2015, the latest in a series of international conferences intended to promote cooperation and discuss norms for responsible behaviour in cyberspace. The desire to develop norms is also evident in the work to develop confidence-building measures through the ASEAN Regional Forum and the Organization for Security and Cooperation in Europe.[45] This essay focuses on two key examples of norm-building activities, tracing the process of norm emergence firstly through the reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), and secondly through US efforts to develop a

norm prohibiting cyber-enabled commercial espionage.

Norm-building in an international forum: The GGE

The GGE has been the preeminent UN vehicle for discussions on issues of stability in cyberspace. The GGE process was set up to examine existing and potential threats in cyberspace and possible cooperative measures to address them. Each group is comprised of twenty states, including the five permanent members of the Security Council. The first group failed to produce a consensus report, after substantial disagreements. However, since then each GGE has produced a consensus report, representing significant steps forward in thinking about international norms for cyberspace. The fifth GGE is currently underway.

The 2010 GGE report highlighted agreement among states that cyber-conflict had become a threat to international peace and stability, and that the lack of international guidance created a risk that a severe cyber incident could spiral into a broader conflict. Accordingly, it recommended dialogue on norms for state use of force in cyberspace, along with confidence-building measures to improve international security and stability.[46] The GGE process has repeatedly emphasised the importance of developing norms for cyberspace. The 2013 report included a landmark consensus that international law, including the UN Charter, applies online as it does offline, but failed to resolve the uncertainties about how it applies (as explored in the preceding section).

The 2014/15 GGE then was specifically tasked with considering "norms, rules or principles for responsible behaviour of States" and "how international law applies to the use of information and communications technologies by States."[47] The report expressed a view that norms are valuable because they "reflect the international community's expectations, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States."[48] More importantly, the 2015 report also made 11 recommendations for new norms and principles, such as a norm that states should not conduct or knowingly support any activity that damages critical infrastructure.[49] While the report explicitly notes that the proposed norms all are voluntary and non-binding, the recommendations are an important step forward in developing an agreed normative framework.

However, whether the GGE reports actually have any norm-setting power is open to question. Subsequent General Assembly resolutions have merely taken note of the reports, and GGE membership is not broadly representative.[50] The 2015 report also failed to make any progress on the application of the LOAC to cyberspace, and China and Russia appear to have backed away from the 2013 agreement that international law applies online.[51] Considering the GGE process through Finnemore and Sikkink's model also highlights that these norms are still at an early point in the cycle. While the 2015 GGE report represents a process of socialisation and active work by norm entrepreneurs, it is not clear yet that a wide range of states have adopted these norms. Nevertheless, the institutionalization of norms through international rules and organisations is often a key step in enabling a norm cascade. The ongoing GGE process may encourage states to adopt these norms by clarifying their content and what constitutes violation.[52]

Bilateral norm-building efforts: Prohibiting cyber-enabled economic espionage

The US can be characterised as a norm entrepreneur in the GGE process and through its bilateral engagement. The 2011 *International Strategy for Cyberspace* included norm-building as a key part of the overall US goal to ensure an open, interoperable, secure and reliable cyberspace, stating that "we will build and sustain an environment in which norms of responsible behaviour guide states' actions, sustain partnerships, and support the rule of law in cyberspace."[53] The *Strategy* emphasised the importance of shared understandings about what constitutes "acceptable" state behaviour to enhance stability and to guide any corrective action.[54] US activity since then is best exemplified by the effort establish a norm prohibiting economically-motivated cyber espionage. Espionage is not illegal under international law. However, the US argues that economic espionage should be treated differently.[55]

The US has repeatedly accused China of large-scale cyber-enabled theft of intellectual property for the benefit of Chinese firms. US officials assert that the scale of Chinese theft has been so massive as to threaten US national and economic security.[56] One study found that "96 percent of recorded, state-affiliated attacks targeting businesses' trade secrets and other intellectual property in 2012 could be traced by to Chinese hackers."[57] In making these

accusations, the US has attempted to distinguish 'unacceptable' cyber-enabled economic espionage from 'acceptable' espionage for national security purposes. The first stage of the norm life cycle is characterised by persuasion by "norm entrepreneurs". These entrepreneurs attempt to persuade a critical mass of states to embrace a new norm.[58] It is possible to trace entrepreneurial efforts by the US through the Obama administration's responses to Chinese economic espionage, both through speech acts and action.

The US has taken punitive actions in support of this emergent norm. For instance, in May 2014, the FBI issued indictments for five officers in the Peoples' Liberation Army on charges including hacking and commercial espionage. While it is highly unlikely that the officers will ever face trial, the US used law enforcement action to send a signal about what it considers constitutes unacceptable behaviour in cyberspace. Reinforcing this, in April 2015, President Obama signed an executive order allowing the US to impose severe financial restrictions on individuals or entities who engage in or benefit from cyber-enabled economic espionage.[59] US officials indicated in August 2015 that the Obama administration was considering issuing a package of these economic sanctions against a range of Chinese actors.[60]

US rhetoric on this issue has also supported its norm-building efforts. China has been publicly named and shamed, and President Obama has described theft of intellectual property and trade secrets as an "act of aggression" and a "core national security threat".[61] This can be contrasted with the US approach to the June 2015 hack of the Office of Personnel Management (OPM), in which up to 22 million personnel details were stolen, including the security clearance information of US government employees. While the OPM hack has been widely attributed to China, the US has not made an official statement to that effect. The refusal to name and shame in this instance reflects a tacit acknowledgment that espionage for national security purposes is a business-as-usual activity. Senior US officials even described the OPM data as a "legitimate foreign intelligence target".[62] The US has actively promoted its proposed norm against economic espionage in an effort to encourage diffusion across the international system.

The second stage of the norm life cycle is a process of imitation and socialisation, as norm entrepreneurs attempt to convince other actors to follow a norm, and for the norm to 'cascade' among international actors. This may happen for a range of reasons, including pressure for conformity and desire for legitimacy.[63] Finnemore and Sikkink describe the primary mechanism for promoting norm cascades as "an active process of international socialization intended to induce norm breakers to become norm followers."[64] The regulative effect of a norm therefore should be observable when a state chooses to abandon an existing policy of resistance and act within the parameters of the norm to avoid the reputational costs of ongoing violation.[65]

China had previously refused to acknowledge any distinction between espionage for national security purposes and economic espionage. Chinese leaders dismissed the 2014 indictments as groundless and did not evidence any feeling that China had violated an international norm.[66] Despite this, Presidents Xi and Obama reached a landmark agreement in September 2015. The two leaders released a joint statement agreeing that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[67] This was an unexpected reversal of the Chinese position, and demonstrates the regulative effect of the emerging norm. The shift in policy may have been for instrumental reasons, given the threat of sanctions. Later in the second stage of Finnemore and Sikkink's model, at a tipping point, enough critical states endorse a norm for that norm to prescribe the appropriate behaviour for an actor with a 'state' identity.[68] The US-China agreement to refrain from cyber-enabled economic espionage was quickly replicated in a range of other agreements, including bilateral statements between China and the UK, China and Germany, and in the November 2015 G20 Leaders' Communiqué.[69]

The final test is the extent to which this norm has been internalised, reconstituting state identities and interests. In the final stage, "norms acquire a taken-for-granted quality and are no longer a matter of broad public debate."[70] Norms come to have a constitutive effect when states choose to comply without any social pressures or strategic reasons to do so. In this instance, US intelligence officials initially saw little change in Chinese behaviour online.[71] More recent reports suggest that breaches attributed to China had dropped by 90 percent over the last two years – most dramatically in the lead up to the September 2015 agreement.[72] Following the G20 in November 2015, US officials

have observed that the international support for the US' peacetime norms has been "remarkable".[73] The bilateral agreements on cyber-enabled economic espionage may provide the impetus for further agreements to emerge, and encourage other states to refrain from the practice.[74]

However, the clandestine nature of cyber threats means that it will be very challenging to monitor compliance with this (or any other) norms for states in cyberspace. The difficulties posed by attribution may also make it far more challenging to prove that a state is breaching a norm. Norms are often tacitly respected even in breach, as states try to justify and defend themselves, or seek to conceal any breach.[75] Communication around a norm can reveal how much it matters.[76] In this context, however, states may not have to defend themselves, as a breach of a cyber security norm may not even be detected, let alone traced back to its source. Moreover, the ability of states to use non-state actors as proxies may also reduce the impact of these norms. The degree to which norms play a role in cyberspace will become clearer in time.

Conclusion

Cyber threats have become widely recognised as a global security issue, emanating within a lawless, anarchic cyberspace. A conscious norm-building project has emerged in response, premised on a collective belief that developing shared understandings on what constitutes appropriate state behaviour in cyberspace is critical to maintain international security and stability. Norm-building efforts in the GGE and in the context of economic espionage highlight the power that norms could have in shaping state behaviour. As these norms emerge and become internalised, they are likely to change state practices in cyberspace. Norms can tame the wild West – not by introducing a sheriff, but through establishing civilised practices.

Bibliography

BBC News, "Sony cyber-attack: North Korea faces new US sanctions," January 3, 2015. Last accessed September 22, 2016. http://www.bbc.com/news/world-us-canada-30661973

Björkdahl, Annika. "Norms in International Relations: Some Conceptual and Methodological Reflections,"*Cambridge Review of International Affairs* 15:1 (2002): 9-23.

Boyer, Dave. "Obama says he doesn't want 'wild West' cyberwar with Russia", *The Washington Times*, September 5, 2016. Last accessed September 8, 2016. http://www.washingtontimes.com/news/2016/sep/5/obama-says-he-doesnt-want-wild-west-cyberwar-russi/

Charney, Scott, et al. *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms.* Microsoft: 2016.

Checkel, Jeffrey T. "The Constructivist Turn in International Relations Theory," *World Politics* 50: 2 (1998): 324:348.

Dahl, Matthew. "Agreements on Commercial Cyber Espionage: An Emerging Norm?" *Lawfare*, December 4, 2015. Last accessed September 5, 2016. https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm

Eichensehr, Kristen. "International Cyber Stability" and the UN Group of Governmental Experts," *Just Security*, July 14, 2015. Last accessed September 5, 2016. https://www.justsecurity.org/24614/international-cyber-stability-un-group-governmental-experts/

Eriksson, Johan and Giampiero Giacomello. "The Information Revolution, Security and International Relations: (IR)relevant Theory?" *International Political Science Review* 27:3 (2006): 221-244.

Erskine, Toni and Madeline Carr. "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace," in *International Cyber Norms: Legal, Policy and Industry Perspectives* eds. Anna Maria Osula and Henry Roigas, 87-109. Tallinn: NATO CCDCOE Publications, 2016.

Finnemore, Martha and Kathryn Sikkink. "International Norm Dynamics and Political Change," *International Organization* 52:4 (1998): 887:917.

Florini, Ann. "The Evolution of International Norms," *International Studies Quarterly*, 40:3 (1996): 363 – 389.

Glanville, Luke. "Does R2P matter? Interpreting the impact of a norm," *Cooperation and Conflict* 51:2 (2016): 184-199.

Hopf, Ted. "The Promise of Constructivism in International Relations Theory," *International Security* 23:1 (1998): 171-200.

Hurwitz, Roger. "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36:5 (2014): 322-331.

Korzak, Elaine. "The 2015 GGE Report: What next for norms in cyberspace?" *Lawfare*, September 23, 2015. Last accessed September 5, 2016. https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace

Lee, Malcolm R. "Will the United States impose cyber sanctions on China?" *Brookings*, September 22, 2015. Last accessed August 26, 2016. http://www.brookings.edu/blogs/order-from-chaos/posts/2015/09/22-will-us-impose-cyber-sanctions-china-lee.

Lewis, James A. "Confidence-building and international agreement in cybersecurity," in *Confronting Cyber Conflict, eds.* Kerstin Vignard, Ross McCrae and Jason Powers, 51-60. Geneva: UNIDIR Disarmament Forum, 2011.

Limbago, Andrea Little. "One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft," *Joint Force Quarterly* 78 (2015): 84-90.

Maness, Ryan C. and Brandon Valeriano. "The Impact of Cyber Conflict on International Interactions," *Armed Forces and Society* (2015): 1-23.

Menn, Joseph and Jim Finkle. "Chinese economic cyber-espionage plummets in U.S.: experts," *Reuters*, June 21, 2016. Last accessed September 21 2016. http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D

Morgus, Robert. "Rules of Cyber Engagement," *Slate*, March 10, 2016. Last accessed September 22, 2016. http://www.slate.com/articles/technology/future_tense/2016/03/the_fuzzy_international_rules_for_war_in_cyberspace.html

Nakashima, Ellen. "U.S. developing sanctions against China over cyberthefts," *The Washington Post*, August 30, 2015. Last accessed September 22, 2016. https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html

Painter, Christopher. "G20: Growing International Consensus on Stability in Cyberspace", *Dipnote*, December 3, 2015. Last accessed September 5, 2016. http://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace

Paletta, Damian. "Former CIA Chief Says Government Data Breach Could Help China Recruit Spies", *The Wall Street Journal*, June 15, 2015. Last accessed August 26, 2016. http://www.wsj.com/articles/former-cia-chief-says-government-data-breach-could-help-china-recruit-spies-1434416996

Schmitt, Michael N. and Liis Vihul. "The Nature of International Law Cyber Norms," Tallinn Paper No.5. Tallinn: Nato Cooperative Cyber Defence Centre of Excellence, 2014.

Segal, Adam. "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement",*Council on Foreign Relations*, January 4, 2016. Last accessed August 26, 2016. http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/

Shalal, Andrea. "Massive cyber attack could trigger NATO response: Stoltenberg," *Reuters,* June 16, 2016. Last accessed September 22, 2016. http://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE

Singer P.W. and Allen Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

United Nations General Assembly Resolution 68/243 "Developments in the field of information and telecommunications in the context of international security," 27 December 2013.

United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, July 22, 2015.

Vaishnav, Chintan, et al. "Cyber international relations as an integrated system," *Environment Systems and Decisions* 33 (2013): 561-576.

Volz, Dustin. "U.S. government concludes cyber attack caused Ukraine power outage," *Reuters*, February 25, 2016. Last accessed September 22, 2016. http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K

The White House, *International Strategy for Cyberspace*. Washington: 2011.

The White House, "FACT SHEET: President Xi Jinping's visit to the United States," September 25, 2015. Last accessed August 26, 2016. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Footnotes

[1] Chintan Vaishnav, et al. "Cyber international relations as an integrated system," *Environment Systems and Decisions* 33 (2013), 563.

[2] Jeffrey T. Checkel, "The Constructivist Turn in International Relations Theory," *World Politics* 50: 2 (1998), 329.

[3] Ted Hopf, "The Promise of Constructivism in International Relations Theory," *International Security* 23:1 (1998), 189.

[4] See Alexander Wendt, "Anarchy is what States Make of It: The Social Construction of Power Politics." International Organisation 46 (1992): 391-425.

[5] Checkel, 329.

[6] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52:4 (1998), 891.

[7] In the interests of clarity, this essay will focus on the role of norms as they affect the behaviour of state actors. However, it is important to note that one of the key features of cyberspace is the multiplicity of actors. Almost all of

the infrastructure underpinning the Internet is owned and operated by the private sector, and the current Internet governance model is based on a multi-stakeholder approach, including states, the private sector, NGOs and civil society. States are not the only actors with a role in determining what constitutes appropriate online behaviour, nor are they the only threat actors in cyberspace.

[8] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security and International Relations: (IR)relevant Theory?" *International Political Science Review* 27:3 (2006), 233.

[9] *Ibid.*

[10] Hopf, 174-5.

[11] Finnemore and Sikkink, 891.

[12] Ann Florini, "The Evolution of International Norms," *International Studies Quarterly*, 40:3 (1996), 364-5.

[13] Toni Erskine and Madeline Carr, "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace," in *International Cyber Norms: Legal, Policy and Industry Perspectives* eds. Anna Maria Osula and Henry Roigas (Tallinn: NATO CCDCOE Publications, 2016), 91.

[14] Annika Björkdahl, "Norms in International Relations: Some Conceptual and Methodological Reflections," *Cambridge Review of International Affairs* 15:1 (2002), 21.

[15] Luke Glanville, "Does R2P matter? Interpreting the impact of a norm," *Cooperation and Conflict* 51:2 (2016), 185.

[16] Glanville, 187.

[17] Matthew Dahl, "Agreements on Commercial Cyber Espionage: An Emerging Norm?" *Lawfare*, December 4, 2015. Last accessed September 5, 2016. https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm

[18] Finnemore and Sikkink, 895.

[19] Glanville, 187-8.

[20] James A. Lewis, "Confidence-building and international agreement in cybersecurity," in, *Confronting Cyber Conflict, eds.* Kerstin Vignard, Ross McCrae and Jason Powers *(*Geneva: UNIDIR Disarmament Forum, 2011), 51.

[21] See for example Myriam Dunn Cavelty, "Cyber-Terror: Looming Threat or Phantom Menace? The Framing of the US Cyber Threat Debate," *Journal of Information Technology and Politics* 4:1 (2008): 19-36.

[22] Quoted in Dave Boyer, "Obama says he doesn't want 'wild West' cyberwar with Russia", *The Washington Times*, September 5, 2016. Last accessed September 8, 2016. http://www.washingtontimes.com/news/2016/sep/5/obama-says-he-doesnt-want-wild-west-cyberwar-russi/

[23] Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions,"*Armed Forces and Society* (2015), 5. Stuxnet successfully targeted the Iranian nuclear programme, damaging centrifuges at the Natanz uranium enrichment plant.

[24] Robert Morgus, "Rules of Cyber Engagement," *Slate*, March 10, 2016. Last accessed September 22, 2016. http://www.slate.com/articles/technology/future_tense/2016/03/the_fuzzy_international_rules_for_war_in_cyberspace.html

[25] Dustin Volz, "U.S. government concludes cyber attack caused Ukraine power outage," *Reuters*, February 25, 2016. Last accessed September 22, 2016. http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K

[26] Examples include the Council of Europe Convention of Cybercrime and Shanghai Cooperation Organisation's International Information Security Agreement. Both have very limited membership and the cybercrime convention a very narrow ambit.

[27] Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," Tallinn Paper No.5, (Tallinn: Nato Cooperative Cyber Defence Centre of Excellence, 2014), 12.

[28] Lewis, 53.

[29] Andrea Shalal, "Massive cyber attack could trigger NATO response: Stoltenberg," *Reuters,* June 16, 2016. Last accessed September 22, 2016. http://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE

[30] The White House, *International Strategy for Cyberspace* (Washington: 2011), 14.

[31] BBC News, "Sony cyber-attack: North Korea faces new US sanctions," January 3, 2015. Last accessed September 22, 2016. http://www.bbc.com/news/world-us-canada-30661973

[32] Lewis, 53.

[33] (New York: Cambridge University Press, 2013).

[34] Schmitt and Vihul, 14.

[35] Andrea Little Limbago, "One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft,"*Joint Force Quarterly* 78 (2015), 90.

[36] Lewis, 52.

[37] Schmitt and Vihul, 19.

[38] *Ibid,* 20.

[39] Lewis, 53.

[40] Lewis, 53.

[41] Scott Charney, et al. *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms* (Microsoft: 2016), 2.

[42] It is worth noting however two competing visions of cyberspace have emerged internationally. The first (largely Western) view is based on an open, secure Internet governed by a wide range of stakeholders. The second (led by China and Russia) focuses on a concept of 'Internet sovereignty', emphasising a multilateral approach to Internet governance and an understanding of information security that includes control of Internet content.

[43] Schmitt and Vihul, 6.

[44] Lewis, 58.

[45] See Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends," in

International Cyber Norms: Legal, Policy and Industry Perspectives eds. Anna Maria Osula and Henry Roigas (Tallinn: NATO CCDCOE Publications, 2016).

[46] Lewis, 54.

[47] United Nations General Assembly Resolution 68/243 "Developments in the field of information and telecommunications in the context of international security," 27 December 2013.

[48] United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, July 22 2015, 7.

[49] UN GGE, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security".

[50] Elaine Korzak, "The 2015 GGE Report: What next for norms in cyberspace?" *Lawfare*, September 23 2015, last accessed September 5 2016. https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.

[51] Kristen Eichensehr, "International Cyber Stability" and the UN Group of Governmental Experts," *Just Security*, July 14, 2015. Last accessed September 5, 2016. https://www.justsecurity.org/24614/international-cyber-stability-un-group-governmental-experts/

[52] Finnemore and Sikkink, 900.

[53] The White House, *International Strategy for Cyberspace*, 8.

[54] *Ibid*, 9.

[55] Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36:5 (2014), 328.

[56] *Ibid*.

[57] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 95.

[58] Finnemore and Sikkink, 895.

[59] See https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.

[60] Ellen Nakashima, "U.S. developing sanctions against China over cyberthefts," *The Washington Post*, August 30, 2015. Last accessed September 22, 2016. https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html

[61] Quoted in Malcolm R. Lee, "Will the United States impose cyber sanctions on China?" September 22 2015, last accessed August 26 2016. http://www.brookings.edu/blogs/order-from-chaos/posts/2015/09/22-will-us-impose-cyber-sanctions-china-lee.

[62] Damian Paletta, "Former CIA Chief Says Government Data Breach Could Help China Recruit Spies",*The Wall Street Journal*, June 15 2015, last accessed August 26 2016. http://www.wsj.com/articles/former-cia-chief-says-government-data-breach-could-help-china-recruit-spies-1434416996

[63] Finnemore and Sikkink, 895.

[64] *Ibid,* 902.

[65] Glanville, 189.

[66] Hurwitz, 328.

[67] The White House, "FACT SHEET: President Xi Jinping's visit to the United States," September 25 2015, last accessed August 26 2016. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[68] Finnemore and Sikkink, 902.

[69] Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement", *Council on Foreign Relations*, January 4, 2016. Last accessed August 26, 2016. http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/

[70] Finnemore and Sikkink, 895.

[71] See for example Mark Hosenball, "U.S. counterintelligence chief skeptical China has curbed spying on U.S." *Reuters*, November 18, 2015. Last accessed August 26, 2016. http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0T72XG20151119

[72] Joseph Menn and Jim Finkle, "Chinese economic cyber-espionage plummets in U.S.: experts," *Reuters*, June 21, 2016. Last accessed September 21, 2016. http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D

[73] Christopher Painter, "G20: Growing International Consensus on Stability in Cyberspace", *Dipnote*, December 3, 2015. Last accessed September 5, 2016. http://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace

[74] Dahl, "Agreements on Commercial Cyber Espionage: An Emerging Norm?"

[75] Erskine and Carr, 91.

[76] Glanville,190.

Written by: Elizabeth Thomas

Written at: Australian National University

Written for: Dr. Cecilia Jacob

Date written: September 2016