Temple University Beasley School of Law
LEGAL STUDIES RESEARCH PAPER NO. 2016-52

Constructing Norms for Global Cybersecurity

Martha Finnemore
George Washington University

Duncan B. Hollis
Temple University Beasley School of Law

November 4, 2016

Cite: 110 American Journal of International Law __ (Forthcoming, 2016)

CONSTRUCTING NORMS FOR GLOBAL CYBERSECURITY

*By Martha Finnemore and Duncan B. Hollis**

On February 16, 2016, a U.S. court ordered Apple to circumvent the security features of an iPhone 5C used by one of the terrorists who committed the San Bernardino shootings.[1] Apple refused. It argued that breaking encryption for one phone could not be done without undermining the security of encryption more generally.[2] It made a public appeal for "everyone to step back and consider the implications" of having a "back door" key to unlock any phone—which governments (and others) could deploy to track users or access their data.[3] The U.S. government eventually withdrew its suit after the F.B.I. hired an outside party to access the phone.[4] But the incident sparked a wide-ranging debate over the appropriate standards of behavior for companies like Apple and for their customers in constructing and using information and communication technologies (ICTs).[5] That debate, in turn, is part of a much larger conversation. Essential as the Internet is, "rules of the road" for cyberspace are often unclear and have become the focus of serious conflicts.

ICTs are now woven into every facet of human activity, from operating nuclear arsenals to raising cows.[6] But for all their benefits, ICTs present an array of new opportunities for causing

* Martha Finnemore is University Professor of Political Science and International Affairs at George Washington University. Duncan B. Hollis is James E. Beasley Professor of Law at Temple University Law School. The authors' research was funded, in part, by a Minerva Grant (No. N00014-13-1-0878) from the U.S. government in cooperation with Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory. The authors thank Jeffrey Dunoff, Virginia Haufler, Alexander Klimburg, Tim Maurer, and participants in the fourth Annual DC IR Workshop for helpful comments, as well as Dalila Berry, Rachel Reznick, and Laura Withers for excellent editorial and research assistance. We are particularly indebted to our late colleague, Roger Hurwitz, of MIT, who introduced the two of us and encouraged us to write this article together. The views expressed are those of the authors alone.

[1] *See* Eric Lichtblau & Katie Benner, *As Apple Resists, Encryption Fray Erupts in Battle*, N.Y. TIMES, Feb. 18, 2016, at A1; Adam Nagourney, Ian Lovett & Richard Pérez-Peña, *Shooting Rampage Sows Terror in California*, N.Y. TIMES, Dec. 3, 2015, at A1.

[2] Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), *at* http://www.apple.com/customer-letter/.

[3] *Id.* The U.S. government insisted that it wanted a new operating system to access a single device, rather than a back door. Cory Bennett, *White House Denies FBI Seeking 'Back Door' to Apple iPhones*, THE HILL (Feb. 17, 2016), *at* http://thehill.com/policy/cybersecurity/269779-white-house-fbi-not-seeking-apple-backdoor-in-terror-case.

[4] *See* Eric Lichtblau & Katie Benner, *F.B.I. Director Suggests Bill for an iPhone Hacking Topped $1.3 Million*, N.Y. TIMES, Apr. 22, 2016, at B3.

[5] Eric Lichtblau, *Security Czars on Apple's Side in Privacy War*, N.Y. TIMES, Apr. 23, 2016, at A1; John Cassidy, *Lessons from Apple vs. the F.B.I.*, NEW YORKER (Mar. 29, 2016), *at* http://www.newyorker.com/news/john-cassidy/lessons-from-apple-versus-the-f-b-i. Use of the term *ICT* is widespread in global cybersecurity. Thus, we use it here notwithstanding that it is often used to refer to international courts and tribunals.

[6] *See* INSTITUTE FOR SECURITY & SAFETY, BRADENBURG UNIVERSITY OF APPLIED SCIENCES, CYBER SECURITY AT NUCLEAR FACILITIES: NATIONAL APPROACHES 2 (June 2015); David Evans, *Introducing the Wireless Cow*, POLITICO (June 29, 2015), *at* http://www.politico.com/agenda/story/2015/06/internet-of-things-growth-challenges-000098.

harm. ICT controls of critical infrastructure, like dams and power grids, may be hacked; personal data, including medical records, may be compromised; and financial assets or intellectual property may be stolen. Cyber *in*security has become the new normal, making cybersecurity a global priority not just for ICT companies but for nation-states, industry, and users generally. As states and stakeholders wrestle over when and how to preserve cybersecurity, they are increasingly turning to norms as the policy tool of choice to ensure cybersecurity for ICTs and cyberspace more generally.[7]

Calls for "cybernorms" to secure and govern cyberspace are now ubiquitous.[8] A UN Group of Governmental Experts[9] (GGE) and a more inclusive "London Process" have campaigned for universal cybernorms for all states.[10] Other cybersecurity efforts target norm development for a limited range of actors (for example, like-minded states,[11] major powers)[12] or in specific interest areas (for example, export controls, data protection).[13]

[7] *Norms* are expectations of proper behavior by actors with a given identity. *See infra* note 85 and accompanying text. As for *cyberspace*, notwithstanding theoretical debates, we understand the concept as the U.S. government does. WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 1 (May 29, 2009), *at* https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (cyberspace refers to the "interdependent network of information technology infrastructures, and includes the Internet, telecommunication networks, computer systems," processors, and controllers embedded in critical industries, as well as to "the virtual environment relating to information and interactions among people").

[8] Hoped-for improvements include (1) deterring unwanted behavior, (2) catalyzing greater cooperation, and (3) improving ICT functionality. *See* Henry Farrell, *Promoting Norms for Cyberspace* 2–3 (Apr. 2015) (Council on Foreign Relations Cyber Brief), *at* http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358; James A. Lewis, *Liberty, Equality, Connectivity—Transatlantic Cooperation on Cybersecurity Norms*, *in* STRATEGIC TECHNOLOGY & EUROPE PROGRAMS, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, LIBERTY, EQUALITY, CONNECTIVITY: TRANSATLANTIC CYBERSECURITY NORMS 7, 8–14 (2014), *at* http://docplayer.net/2023317-Liberty-equality-connectivity-transatlantic-cooperation-on-cybersecurity-norms.html; Roger Hurwitz, *A New Normal? The Cultivation of Global Norms as Part of a Cyber Security Strategy*, *in* CONFLICT AND COOPERATION IN CYBERSPACE: THE CHALLENGE TO NATIONAL SECURITY 213 (Panayotis A. Yannakogeorgos & Adam B. Lowther eds., 2013).

[9] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paras. 9–15, UN Doc. A/70/174 (July 22, 2015) [hereinafter 2015 GGE Report].

[10] Formally, the Global Conference on CyberSpace. *See* https://www.gccs2015.com.

[11] By way of examples, (1) the Shanghai Cooperation Organization has produced two international codes of conduct for information security, (2) the Council of Europe sponsored the Budapest Convention on Cybercrime, and (3) NATO funded an independent group of experts to author the *Tallinn Manual* on the international law applicable to cyberwar. *See*, *e.g.*, International Code of Conduct for Information Security, *in* Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, UN Doc. A/69/723, annex (Jan. 9, 2015) [hereinafter Revised SCO Code of Conduct]; Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS No. 185 [hereinafter Budapest Convention]; TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

[12] *See*, *e.g.*, White House Press Release, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), *at* https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (U.S.-China deal on commercial cyberespionage); Agreement Between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in Ensuring International Information Security, May 8, 2015 [hereinafter Russia-China Agreement] (unofficial English translation available at http://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf).

[13] *See*, *e.g.*, Wassenaar Arrangement, *at* http://www.wassenaar.org (export controls regarding intrusion software and IP network surveillance systems); European Commission Press Release, Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market (Dec. 15, 2015), *at* http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

These cybernorm projects share a common theme. They conceptualize norms as *products*, focusing on what norms should say rather than how they will work.[14] What norms say—their substantive content and the behavioral expectations that they set—is certainly important. There are, moreover, plenty of disagreements to hash out, including whether encryption back doors are appropriate. But even if these projects agreed on what cybernorms should say, simply pronouncing them is unlikely to have the desired effects.[15] That is not how norm cultivation works. Norms are not deracinated abstractions; they do not come about by fiat or desire, and they are never imposed in a vacuum. Norms are social creatures that grow out of specific contexts via social processes and interactions among particular groups of actors. Understanding both those contexts and those processes is as important to successful norm construction as agreeing on content.

Efforts to construct new and better cybernorms must start by accommodating or at least recognizing the existing contexts in which norms are sought.[16] There is no blank slate from which to work on cybersecurity. Cyberspace already has a robust and diverse array of norms. National regulations, international laws, professional standards, political agreements, and technical protocols litter the cybersecurity terrain, all involving substantial normative commitments in various stages of development and diffusion. This existing landscape shows that cybersecurity is not a unified problem set; cybernorms have no single "context." Instead, the ICT landscape presents a diverse array of problems rooted in diverse communities of actors—a heterogeneity that requires diverse normative solutions. Norms for securing the integrity of Internet domain names present an entirely different set of issues from those involved in protecting a firm's networks, let alone those for securing critical infrastructure from a military cyber-operation.

Beyond context, the real power of norms (and much of their attraction as a regulatory tool) lies in the *processes* by which they form and evolve. The success of a norm rests not just in what it says, but in who accepts it, not to mention where, when, and how they do so. It matters to the content and future of a norm, for example, whether it is promulgated by states at the United Nations, technologists in an industry association, privacy activists in a nongovernmental organization (NGO), or some freestanding multistakeholder group open to all these actors. Fortunately, the social science literature has already explored a diverse array of norm-construction processes. That literature offers useful lessons missed if one examines cybernorms only as products. Indeed, existing research strongly challenges

[14] For notable exceptions, see, for example, Microsoft Corp., *Five Principles for Shaping Cybersecurity Norms* 8–10 (2013), *at* http:/www.microsoft.com/en-au/search/result.aspx?q=Five+Principles+for+Shaping+Cybersecurity+Norms&form=dlc; GREG AUSTIN, BRUCE MCCONNELL & JAN NEUTZE, EASTWEST INSTITUTE, PROMOTING INTERNATIONAL CYBER NORMS: A NEW ADVOCACY FORUM 4–9 (2015), *at* https://cybersummit.info/sites/cybersummit.info/files/BGCyberNorms_FINAL.pdf; Kristen E. Eichensehr, *The Cyber-law of Nations*, 103 GEO. L.J. 317, 361–64 (2015).

[15] For example, even if U.S. courts or Congress requires companies like Apple to include back-door capacities to decrypt in response to a warrant, the United States remains just one state, and Apple—like other ICTs—operates globally. *See* Andrea Peterson, *The Debate over Government 'Backdoors' into Encryption Isn't Just Happening in the U.S.*, WASH. POST: THE SWITCH (Jan. 11, 2016), *at* https://www.washingtonpost.com/news/the-switch/wp/2016/01/11/the-debate-over-government-backdoors-into-encryption-isnt-just-happening-in-the-u-s/.

[16] Toni Erskine & Madeline Carr, *Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace*, *in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES 87, 88 (Anna-Maria Osula & Henry Rõigas eds., 2016) (calling for analysis of existing context and distinguishing proposed—or "quasi"—norms from those with prescriptive force).

the idea that states and stakeholders can "settle" on any set of cybernorms, providing fixed expectations for future behavior. Norms have an inherently dynamic character; they continuously develop via ongoing processes in which actors extend or amend their meaning as circumstances evolve. This suppleness is part of their attraction, but managing this dynamism also requires foresight currently lacking among those seeking to construct cybernorms.

In this article we reorient the existing conversation by offering a *process*-centered analysis of cybernorms, one that foregrounds how norms work and that complements existing debates over what they say. We do so in four steps. In part I, we "map" the cybersecurity problem. We illustrate the economic, humanitarian, and national security stakes involved and explore the varied contexts that create diverse cybersecurity challenges. In part II, we introduce the norm concept and examine the elements that make up any norm. Drawing on the (now rich) social science literature, we offer a *process*-focused analysis of catalysts for norm creation—entrepreneurship and changed habits—along with key tools to help norms take root and spread: incentives, persuasion, and socialization. We explain key aspects of norm dynamics—how norms arise, spread, and change—and the multiple ways that they are cultivated and interact with other norms.

In part III, we examine the claim that cyberspace is a unique regulatory arena such that lessons about norms from other domains may not apply. Specifically, we evaluate claims that cyberspace is unique because of its (1) technical architecture (ICT's speed, scale, and potential for secrecy) and (2) governance structures (autonomy from sovereign control, the regulatory role of code, and "multistakeholder governance"). We find that, on balance, none of these characteristics disqualify cyberspace from our process-oriented analysis or exempt cybernorms from the general characteristics of norm dynamics. Claims about cyberspace's novelty often prove either inaccurate or overstated. Even when cyberspace *is* an outlier (for example, the speed of ICT development), we are reluctant to conclude that this fact alone pushes cybernorms beyond, rather than along, the existing spectrum of global norm processes.

Our fourth (and most important) step examines the strategic choices faced in pursuing new cybernorms. In part IV, we situate the extant focus on *what* cybernorms say within the larger set of decisions that actors make in constructing cybernorms, including (1) what problems need addressing, (2) which norm components should make up the desired norm process, and (3) what promotion and socialization tools should be deployed to make the norm effective. The answers to these questions can affect the successful formation and diffusion of cybernorms as much as their contents. A decision to "graft" new cybernorms onto existing institutions (as is happening, for example, with the Wassenaar Arrangement's inclusion of cybersecurity technology) presents a different set of possibilities and problems than one where states or stakeholders set up a new process like the NETmundial Initiative.[17] We thus identify some of the most likely trade-offs involved in each of these strategic choices.

These choices are not exclusive; states and stakeholders can and do pursue norms simultaneously through multiple pathways. Further, whatever results these processes generate, we expect outcomes to remain inherently dynamic. Cybernorms will continue to evolve

[17] *See* Wassenaar Arrangement, *supra* note 13; *NETmundial Multistakeholder Statement* (Apr. 24, 2014), *at* http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

as new cases (and new technologies) require actors to reinterpret their cybernorms accordingly. More importantly, to the extent that actors in cyberspace identify with multiple groups or fulfill multiple roles, we anticipate that cybernorms will operate alongside other norms in varying contexts, without clear hierarchies or processes for resolving conflicts.

In this article we do not express a preference for or otherwise privilege any particular strategic choice(s) for future cybernorms. Indeed, we do not even go so far as to predict that process-related choices will generate reliable (let alone effective) normative outcomes. Failure remains an option (and may even be the dominant outcome). The goals of this article are more modest. Our central claim is simply that the journey matters as much as the destination—that how cybernorms are constructed will shape the content and character of the norms that emerge. States and other stakeholders thus need to think more carefully than they have to date about *how* norms evolve, spread, and affect behavior.

Our process-centered analysis has both practical and theoretical implications. By showing the stakes involved in cybernorm process choices, our article offers constructive advice to states and stakeholders in their efforts to secure cyberspace. At the same time, our work offers new insights into both international relations and international law. For international relations, which has a deep familiarity with norms, we offer new insights about possibilities for "strategic social construction" around this bedrock technology in our connected and globalized world.[18] Much of the norms scholarship within international relations has focused on the promotion of well-articulated individual norms for specific actors who know what they want. The cyber context, by contrast, forces us to think more seriously about norm construction in situations of rapid change that make preferences fluid and where potential tensions or trade-offs exist among interdependent norms.

For international law, our work provides an analytical frame for understanding the mechanisms on which international law must rely to achieve its (often unspoken) goal—namely, the creation and instantiation of norms for its subjects. In doing so, we also offer a more nuanced take on the potential for "nonlaw" to effectively govern global problems. Proponents of soft law have long trumpeted the compliance pull of non–legally binding "norms," but to date, international law as a discipline has given relatively little attention to the processes by which such norms garner authority. Our work presents an opportunity to do so in an area that has become one of the most pressing problems of global governance.

I. CYBERSECURITY: THE WORLD OF CYBERNORMS

In 2012, a cybersecurity breach at Saudi Aramco, the world's largest oil producer, altered prices for hard drives across the globe.[19] On August 15, most employees were on

[18] *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 909–15 (1998).

[19] *See* Jose Pagliery, *The Inside Story of the Biggest Hack in History*, CNN MONEY (Aug. 5, 2015), *at* http://money.cnn.com/2015/08/05/technology/aramco-hack/; Fahmida Y. Rashid, *Inside the Aftermath of the Saudi Aramco Breach*, DARKREADING (Aug. 8, 2015), *at* http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676?print=yes.

vacation for Ramadan when a self-replicating virus, dubbed "Shamoon," struck the company's Windows-based systems.[20] Shamoon exfiltrated files on infected computers to an unknown external server before wiping the computers clean and rendering them inoperable.[21] Employees had to unplug every computer and disconnect their data centers. Before they finished, nearly three-quarters of Saudi Aramco's computers—thirty-five thousand in all—were partially wiped or totally destroyed.[22] A group calling itself the "Cutting Sword of Justice" claimed responsibility. Media reports fingered Iran, suggesting Shamoon was reverse engineered from the Stuxnet malware that had previously infected Iranian systems.[23]

Shamoon left the company's business processes in tatters (it did not infect industrial-control systems managing oil production). Saudi Aramco lost its ability to make payments, manage supplies, and track shipments.[24] Domestic oil distribution halted for seventeen days, leading to gas shortages and miles-long lines of empty tanker trucks waiting for gas (which the company ended up giving away for free for a short time). To replace its computers, Saudi Aramco used private jets to fly employees to factory floors in Southeast Asia with orders to buy up every hard drive available, leading to the aforementioned global price rise.[25] In the end, it took Saudi Aramco five months to bring business processes back on line.[26]

The Shamoon virus—including its impact on Saudi Aramco's finances, its business secrets, and hardware prices—provides a dramatic illustration of the need for cybersecurity. It is, however, just a single example. Global cybersecurity implicates a tremendous range of economic, privacy, and national security issues. Estimated global losses from cybercrime now exceed U.S.$400 billion per year.[27] Privacy problems are on a similar scale; 2015 witnessed the loss of seven hundred million records of personal data.[28] Hacks like those that identified users of

[20] Rashid, *supra* note 19.

[21] *The Shamoon Attacks*, SYMANTEC OFFICIAL BLOG (Aug. 16, 2012), *at* http://www.symantec.com/connect/blogs/shamoon-attacks.

[22] Pagliery, *supra* note 19.

[23] Nicole Perlroth, *Cyberattack on Saudi Firm Disquiets U.S.*, N.Y. TIMES, Oct. 24, 2012, at A1; Kim Zetter, *The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks*, WIRED (Feb. 10, 2015), *at* https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/. Stuxnet is widely assumed to be a state-sponsored form of malware. Discovered in 2010, it infected similar systems worldwide but executed only on Iran's Natanz facility, leaving other systems unharmed (although still requiring a patch once the virus became known). KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON 354–58 (2014); RONALD J. DEIBERT, BLACK CODE: SURVEILLANCE, PRIVACY, AND THE DARK SIDE OF THE INTERNET 176–80 (2013); Ralph Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, 9 IEEE SECURITY & PRIVACY 49, 49–50 (2011).

[24] Rashid, *supra* note 19; *see* Christopher Bronk & Eneken Tikk-Ringas, *The Cyber Attack on Saudi Aramco*, 55 SURVIVAL 81, 85–88 (2013).

[25] A flood in Thailand may also have contributed to demand. David Goldman, *Thailand Floods Could Create Laptop Shortage*, CNN MONEY (Nov. 1, 2011), *at* http://money.cnn.com/2011/11/01/technology/thailand_flood_supply_chain/.

[26] Rashid, *supra* note 19; Pagliery, *supra* note 19.

[27] CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 6 (June 2014), *at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[28] *See*, *e.g.*, *Gemalto Releases Findings of 2015 Breach Level Index* (Feb. 23, 2016), *at* http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2015-Breach-Level-Index.aspx.

the marital infidelity site *Ashley Madison*[29] or that compromised U.S. Office of Personal Management (OPM) databases illustrate just how intrusive privacy losses can be.[30] U.S. assertions of Chinese responsibility for the OPM hack show, moreover, how data breaches implicate national security.[31] Of course, states themselves are also often interested in compromising cybersecurity, whether for the intelligence purposes revealed by Edward Snowden, the coercive goals of North Korea's hack of Sony Pictures,[32] or the kinetic damage that Stuxnet caused at Iran's Natanz uranium enrichment facility.[33]

Given such diversity of modes and methods of damage associated with the term *cybersecurity*, it is not surprising that definitions can vary.[34] For our purposes, we define cybersecurity simply as *the protection of information and communication technologies from unauthorized access or attempted access.*[35] Doing so cabins our subject in two key ways. First, the idea of *unauthorized* access implies the presence of an adversary, thus capturing *intentional* threats (for example, cyberattacks) while excluding *unintentional* ones (for example, internal computer errors or interoperability problems).[36] Second, by emphasizing the protection of ICT itself, we exclude security issues associated with the content of ICT communications (for example, subversive online speech or child pornography). We do not mean to suggest that these are unimportant topics. Both constitute serious problems capable of causing real harms and disruption.[37] Yet, we forgo addressing them here for pragmatic reasons. Even under our simple definition, cybersecurity is a heterogeneous policy problem in which threats have varying causes, effects, and authors.

[29] Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015), *at* http://fortune.com/2015/08/26/ashley-madison-hack/.

[30] *See* U.S. Office of Personnel Management, Cybersecurity Resource Center, *at* https://www.opm.gov/cybersecurity/. The OPM compromise included security-clearance and background-check information for 21.5 million former and current federal employees and contractors, including data such as drug and alcohol habits, criminal history, and marital troubles. *Id.*; Michael Adams, *Why the OPM Hack Is Far Worse Than You Imagine*, LAWFARE (Mar. 11, 2016), *at* https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine; *Ex-NSA Officer: OPM Hack Is Serious Breach of Worker Trust*, NPR (June 13, 2015), *at* http://www.npr.org/2015/06/13/414149626/ex-nsa-officer-opm-hack-is-serious-breach-of-worker-trust.

[31] Julianne Pepitone, *China Is 'Leading Suspect' in OPM Hacks, Says Intelligence Chief James Clapper*, NBC NEWS (June 25, 2015), *at* http://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881.

[32] *See*, *e.g.*, Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST: THE SWITCH (Dec. 18, 2014), *at* https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

[33] Stuxnet interfered with industrial control systems at Natanz by instructing centrifuges to run at various—and unsustainable—speeds. ZETTER, *supra* note 23, at 341–42; Langner, *supra* note 23, at 50.

[34] For more cybersecurity definitions, see Cyber Security Initiative, *Global Cyber Definitions Database*, NEW AMERICA, *at* http://cyberdefinitions.newamerica.org.

[35] This definition tracks loosely one that the U.S. government previously used. *See* U.S. Department of Defense, *Instruction No. 5205.13: Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities* 10 (Jan. 29, 2010), *at* http://www.dtic.mil/whs/directives/corres/pdf/520513p.pdf. More recent U.S. definitions have become unwieldy. *See* "cybersecurity," Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies, *A Glossary of Common Cybersecurity Terminology*, *at* https://ics-cert.us-cert.gov/sites/default/files/documents/Common%20Cyber%20Language_S508C.pdf.

[36] *Accord* P. W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 34 (2014); NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, GLOSSARY OF KEY INFORMATION SECURITY TERMS 57–58 (Richard Kissel ed., 2013), *at* http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[37] *See*, *e.g.*, Nathaniel Popper, *The Bell Rings, Computers Fail, Wall St. Cringes*, N.Y. TIMES, July 9, 2015, at A1; Christopher Drew, *United Halts Fights for 2 Hours, Blaming Faulty Network Equipment*, N.Y. TIMES, July 9, 2015, at B2. For online speech controls, China is the paradigmatic example. Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah Mckune, Arn Rey, John Scott-Railton, Ronald Deibert & Vern Paxson, *China's Great Cannon*, CITIZEN LAB (Apr. 10, 2015), *at* https://citizenlab.org/2015/04/chinas-great-cannon/.

The Causes of Cyber Insecurity

The threats encompassed by our cybersecurity definition are created by three elements: (1) knowledge of a vulnerability, (2) access to it, and (3) a payload.[38] All cyber insecurities require some vulnerability—that is, a flaw or weakness that makes the ICT susceptible to penetration by an outside actor. Given the millions of lines of code involved in modern programming, vulnerabilities are an inherent feature of cyberspace. They arise, moreover, across all the layers in which ICTs operate, from applications like Apple's iTunes software to the routers that send data packets across the Internet.[39]

A cybersecurity threat begins once an adversary learns about a vulnerability. Many vulnerabilities are documented and cataloged, with the consequence that users can minimize exposure.[40] More rarely, adversaries discover vulnerabilities of which there was no prior knowledge. These are referred to as *zero-day* vulnerabilities because defenders have no time (that is, zero days) to defend against them. A black market has emerged for trading in zero-day vulnerabilities.[41] Some vendors sponsor "bug bounty programs" to recognize and compensate researchers who responsibly disclose zero-day vulnerabilities in lieu of turning to the black market. All actors, including states, who learn of such vulnerabilities must choose whether to disclose the vulnerability or use it for their own purposes.[42]

Of course, adversaries must not simply know about a vulnerability in a target's ICT; they must also have access to it. The layered and distributed nature of ICT affords multiple access vectors, including: (1) *remote access*, or "hacking," which can originate from anywhere with an Internet connection; (2) *supply chain access* via back doors built into hardware or software during their creation or servicing; (3) *denial of access*, such as a "distributed denial of service" (DDoS) attack, in which data requests flood a website's server, overwhelming its ability to respond or process data, effectively disabling it for everyone (including legitimate traffic);[43] (4) *proximity access*, in which physical proximity to machinery or wi-fi gives adversaries opportunities to connect to the same network or convince unsuspecting targets to make the connection for them; and (5) *insider access*, whether

[38] Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 64 (2010).

[39] ICT functions fall broadly into four layers. A bottom "link" layer includes the physical media allowing transmission of data packets. Next are the "network" and "transport" layers; the "network" layer breaks data into packets with their source and destination identified via an addressing system of "headers." The "transport" layer ensures reliable transmission of data packets, routing them from one network to another. At the top of the stack, the "applications" layer converts data into useful things like Web pages or files. Each layer functions independently; Google Chrome works regardless of whether the link layer employs DSL or wi-fi. For a further—and more precise—account, see *The OSI Model's Seven Layers Defined and Functions Explained*, MICROSOFT CORP. (2014), *at* http://support.microsoft.com/kb/103884.

[40] *See* National Institute of Standards & Technology, *National Vulnerability Database, at* https://nvd.nist.gov. Because many users fail to patch their systems, these vulnerabilities still constitute serious security risks.

[41] Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, WIRED (Apr.17, 2015), *at* https://www.wired.com/2015/04/therealdeal-zero-day-exploits/.

[42] The Federal Bureau of Investigation, for example, used a zero-day vulnerability to catch people using online child pornography sites. Ellen Nakashima, *In War on Child Porn, FBI Borrows Hackers' Techniques*, WASH. POST, Jan. 22, 2016, at A3.

[43] DDoS attacks often occur via "botnets," networks of compromised computers culled together to do the bidding of an unauthorized remote user, often without the owner's knowledge. SINGER & FRIEDMAN, *supra* note 36, at 44.

provided willingly by disgruntled insiders like Edward Snowden or unwittingly through social-engineering techniques like *spearphishing*.[44]

Cybersecurity experts do not worry about vulnerabilities (or access to them) for their own sake. Their chief concern is the "payload" that an adversary with access may deploy to exploit the designated vulnerability. Payloads take many forms, including viruses, worms, and Trojan horses.[45] They may be selective and target specific high-value targets, or indiscriminate, like the Heartbleed virus, and exploit all ICTs to which access can be gained.[46]

The Effects of Cyber Insecurities

For computer scientists, the effects of cyber insecurity have traditionally involved one or more elements of the "CIA" triad: losses of (1) confidentiality, (2) integrity, and (3) availability.[47] For regulators, however, the effects that generate the most concern are (4) the indirect ones.

Confidentiality losses involve payloads, or "exploits," that access data found in, or transiting through, ICT that was otherwise intended to remain private.[48] The affected data can be financial (like the 110 million credit card numbers stolen from Target in 2013) or more personal (like that lost in the OPM hack).[49] The term *cyberattacks* refers to payloads that do more than access data; they affect the *integrity* of ICT functions. Cyberattacks interfere with how ICTs work, by modifying, supplanting, or destroying the data resident on such systems. Both Shamoon and Stuxnet involved integrity losses. Losses of ICT *availability* deny users access to ICT itself. In the spring of 2007, for example, Estonia famously fell victim to a massive DDoS attack that, for several weeks, severely degraded much of the country's online presence, including websites of its parliament, government ministries, banks, hospitals, and media outlets.[50] Availability losses may also accompany "ransomware" attacks that restrict a user's access to an

[44] In spearphishing, an adversary poses as a trusted party to induce the victim to introduce malware into his or her network (such as by opening an email attachment). The Shamoon virus accessed Saudi Aramco's networks via spearphishing. Candid Wueest, *Security Response: Targeted Attacks Against the Energy Sector* 12–14, SYMANTEC (2014), *at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf; Rashid, *supra* note 19.

[45] Viruses spread by attaching themselves to programs or files and cannot infect a computer unless users open the program or file. Worms self-replicate, spreading without human interaction. Trojan horses are seemingly innocent programs containing malware. Rootkit programs allow hackers access to computer functions as administrators while remaining hidden from operating systems and antivirus software. MOHAMED CHAWKI, ASHRAF DARWISH, MOHAMMAD AYOUB KHAN & SAPNA TYAGI, CYBERCRIME, DIGITAL FORENSICS AND JURISDICTION 39–51 (2015); *A Glossary of Common Cybersecurity Terminology*, *supra* note 35 (defining "rootkit").

[46] *See* Joseph Steinberg, *Massive Internet Security Vulnerability—Here's What You Need to Do*, FORBES (Apr. 10, 2014), *at* http://www.forbes.com/sites/josephsteinberg/.

[47] Mohammad Nazmul Alam, Subhra Prosun Paul & Shahrin Chowdhury, *Security Engineering Towards Building a Secure Software*, 81 INT'L J. COMPUTER APPLICATIONS 32, 33–34 (2013).

[48] Lin, *supra* note 38, at 67–68.

[49] *See* Anthony Wing Kosner, *Actually Two Attacks in One, Target Breach Affected 70 to 110 Million Customers*, FORBES (Jan. 17, 2014), *at* http://www.forbes.com/sites/anthonykosner/; *supra* note 30 and accompanying text (re: OPM).

[50] *See*, *e.g.*, Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at C7; Steven Lee Myers, *Estonia Computers Blitzed, Possibly by the Russians*, N.Y. TIMES, May 19, 2007, at A8.

ICT system until a ransom is paid; these attacks can affect anyone from grandmothers to gambling sites.[51]

But the most significant effects of cyber insecurities are *indirect*. Losses of confidentiality, integrity, and availability are usually designed with some other effect(s) in mind. Stuxnet's goal was not simply to breach the integrity of Natanz's industrial-control systems but to use that compromise to run centrifuges at unsustainable speeds, causing a thousand of them to self-destruct and thereby setting back Iran's nuclear ambitions.[52] In 2015, researchers demonstrated that compromising a Jeep's ICT could allow attackers to cut off its engine.[53] Most recently, malware took parts of Ukraine's power grid off-line, raising concerns about the knock-on effects to life and property that accompany a loss of power.[54]

Each of these effects—concerning confidentiality, integrity, availability, and indirect consequences—may occur in isolation or in concert. Losses may start the moment that access occurs or may await a particular triggering date or condition (which are a key feature of "logic bombs").[55] Once activated, effects can last nanoseconds or persist for years.[56] Losses may be immediately obvious or remain surreptitious, such that a victim may not be aware of the loss of confidentiality or may write off integrity effects as the result of internal error. As a result, an adversary now operates, on average, for 205 days within a victim's system before detection.[57]

Even after detection, victims may not know what effects an intrusion risks. The pathways for exploiting confidentiality are the same as those for attacking the integrity of a system or network.[58] Thus, it can be technically difficult to know what capabilities any particular piece of malware has: will it only collect data or might it at some point alter or wipe a system? Ultimately, the consequences of any cyber insecurity turn on resilience: the victim's capacity to operate in a degraded state or the speed at which it can remediate the losses suffered.

Cataloging the Authors of Cyber Insecurity

Who would want to perpetrate these kinds of attacks? For our purposes, four categories of potential authors bear special mention: (1) hackers, (2) hacktivists, (3) organized criminals,

[51] *See* Alina Simone, *How My Mom Got Hacked*, N.Y. TIMES, Jan. 4, 2015, at SR1, *at* http://www.nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-hacked.html; Thomas Fox-Brewster, *How Hackers Breached Two Gambling Payment Providers to Harvest 'Millions' of Records*, FORBES (Nov. 5, 2015), *at* http://www.forbes.com/sites/thomasbrewster/. Recently, ransomware has targeted entire hospital networks. Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016), *at* https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

[52] ZETTER, *supra* note 23, at 341–42, 363.

[53] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—with Me in It*, WIRED (July 21, 2015), *at* https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[54] *See* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid,* WIRED (Mar. 3, 2016), *at* https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[55] Logic bombs are programs hidden within seemingly innocuous programs that execute their payloads at a specified time or when certain conditions are met.

[56] The exploit "Titan Rain" persisted for at least three years. James A. Lewis, *Computer Espionage, Titan Rain and China*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (Dec. 2005), *at* https://www.csis.org/analysis/computer-espionage-titan-rain-and-china; Bradley Graham, *Hackers Attack via Chinese Web Sites, U.S. Agencies' Networks Are Among Targets*, WASH. POST, Aug. 25, 2005, at A1.

[57] MANDIANT THREAT REPORT: M-TRENDS 2015: A VIEW FROM THE FRONT LINES 3 (2015), *at* https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf. This figure represents an improvement from earlier years. *See id*.

[58] Lin, *supra* note 38, at 82.

and (4) states. Individual hackers penetrate computer systems to demonstrate technical capacities or their skills. The stereotype of a basement-dwelling teenager hacker may be outdated,[59] but the capacity of hackers with sufficient expertise to cause significant losses remains.[60] "Hacktivists" differ from hackers in that they pursue cyber insecurity to advance a specific cause, whether concerning a country, government, ideology, or issue. For example, hacktivists targeted Estonia with the 2007 DDoS to punish that country for its perceived mistreatment of Russia.[61] More recently, the hacktivist collective Anonymous has targeted and taken down ISIS social media platforms, while ISIS has its own online supporters who recruit fighters and release personal information about U.S. service members.[62]

Like hacktivists, cybercriminals have organized into groups, but they author cyber exploits and attacks primarily for the promise of financial gains. Cybercriminals notoriously operate transnationally, taking advantage of territorial constraints on the ability of states to prescribe, let alone enforce, criminal laws beyond their borders.[63] This is not to say that cybercriminals always operate with impunity. China, for example, has arrested several individuals within its territory that it alleges authored the OPM hack (although U.S. officials are reportedly skeptical that the OPM intrusion was the work of individual hackers).[64]

Finally, states themselves may author cyber exploits and attacks. Intelligence agencies or their proxies may deploy exploits to gather data on everything from foreign officials to corporations and individual users.[65] Dozens of countries now have their own cyberforces, including U.S. Cyber Command.[66] Militaries have indicated that they may pursue cyber-operations to supplement traditional force, as Russia did in 2008 in Georgia.[67] Or militaries may plan stand-alone operations doing things that kinetic weapons never could—for example, disabling a power grid instead of blowing it up (as Russia may have done to Ukraine in 2015).[68]

Attributing responsibility for a cyber-incident to one of these four categories of actors (let alone the actual perpetrator) poses a serious challenge. Known as the "attribution problem," the layered and distributed nature of ICT often allows sophisticated actors to maintain their

[59] *But see* Darren Boyle, *British Teenager Was Part of Team of Hackers Who Caused Government Websites in The UK and USA to Crash*, DAILY MAIL (Aug. 19, 2015), *at* http://www.dailymail.co.uk/news/article-3203894/British-teenager-team-hackers-caused-government-websites-UK-USA-crash.html.

[60] *See* Kim Zetter, *Feds Say That Banned Researcher Commandeered a Plane*, WIRED (May 15, 2015), *at* https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

[61] Myers, *supra* note 50. The DDoS began after Estonia relocated a World War II memorial to Russian war dead. *Id.*

[62] *See*, *e.g.*, Ashley Fantz, *As ISIS Threats Online Persist, Military Families Rethink Online Lives*, CNN (Mar. 23, 2015), *at* http://www.cnn.com/2015/03/23/us/online-threat-isis-us-troops/; Don Reisinger, *Anonymous Declares Cyber War on ISIS. Why It Matters*, FORTUNE (Nov. 16, 2015), *at* http://fortune.com/2015/11/16/anonymous-cyber-war-isis/.

[63] *See* Kaveh Waddell, *FBI's Most Wanted Cybercriminals*, ATLANTIC (Apr. 27, 2016), *at* http://www.theatlantic.com/technology/archive/2016/04/the-fbis-most-wanted-cybercriminals/480036/.

[64] Ellen Nakashima, *China: Hackers' Arrested*, WASH. POST, Dec. 3, 2015, at A3.

[65] *See NSA Targets World Leaders for US Geopolitical Interests*, WIKILEAKS (Feb. 23, 2016), *at* https://wikileaks.org/nsa-201602/.

[66] Wesley R. Andrues, *What U.S. Cyber Command Must Do*, 59 JOINT FORCES Q. 115 (2010); DEIBERT, *supra* note 23, at 183; Jennifer Valentino-Devries & Danny Yadron, *Cataloging the World's Cyberforces*, WALL ST. J. (Oct. 11, 2015), *at* http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

[67] *See* John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1.

[68] *See* Zetter, *supra* note 54.

anonymity.[69] Attackers can even disguise their efforts so that they appear to originate with some other group or government.[70] This ability to "false flag" provides accused actors with a ready-made defense, insisting that they have been framed, no matter the evidence against them. Russia took this path when Estonia accused it of having orchestrated the 2007 DDoS attack, as did North Korea in response to U.S. allegations that it hacked Sony Pictures.[71]

Even with technical attribution, however, responsibility issues persist because of the malleability among author categories. Individuals can easily shift camps (or belong to more than one simultaneously). A hacker may disclose vulnerabilities regularly and yet sell one on the black market for the money. States can operate in cyberspace directly but also via proxies, encouraging or even directing behavior by hacktivists or cybercriminals. China's stance on the OPM hack suggests the inverse possibility, in which responsibility is attributed to a state when the actual authors are cybercriminals operating from within an unknowing state's apparatus.[72]

Such diverse causes, effects, and authors of cyber insecurity require a diverse array of security measures. The problem of zero-day markets is different than educating users about the dangers of spearphishing. Data breaches are a real (and growing) problem, but they should not be conflated with the loss of power that can follow a breach of integrity on a nation's power grid. And, of course, how one thinks about (let alone attempts to regulate) such losses very much depends on whether the author is a lone-wolf hacker or one of the most powerful nation-states in the world.

Managing such a varied array of cyber insecurities is a daunting challenge that has generated heated debate. One point of consensus, however, is that cultivating new and better norms of behavior for cyberspace is an essential component of any cybersecurity strategy. But how can norms help alleviate these many cybersecurity threats? How can useful norms be created to accomplish the desired goals? Attention to the varied ICT contexts is an obvious starting point. Constructing cybernorms, however, requires more than understanding the problems faced; we must also understand what norms are and how they work.

II. NORMS AND THEIR PROCESSES

Today, norms have become the preferred regulatory vehicle for advancing the stability and safety of cyberspace. The United States emphasized in its *International Strategy for Cyberspace*

[69] *See* Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), *at* http://www.scientificamerican.com/article/tracking-cyber-hackers/; HOWARD F. LIPSON, TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES 13–15 (Nov. 2002), *at* http://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf. Technical attribution is not impossible but takes time and skill. Attribution may also come from secondary intelligence, mistakes, or luck. Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L. L.J. 373, 397–401 (2011); *see also infra* notes 196–203 and accompanying text.

[70] MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 44 (2009). Nor have assumptions about authors based on the type of attack proved reliable. *See* Kim Zetter, *Israeli Hacker 'The Analyzer' Indicted in New York—Update*, WIRED (Oct. 29, 2008), *at* https://www.wired.com/2008/10/israeli-hacker (noting three teenagers perpetrated "Solar Sunrise" exploit, which the United States had mistakenly assumed was state organized).

[71] Landler & Markoff, *supra* note 50 (re: Russia); Jack Kim & Steve Holland, *North Korea Denies Hacking Sony, U.S. Stands by Its Assertion*, REUTERS (Dec. 20, 2014), *at* http://www.reuters.com/article/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141220.

[72] *See supra* note 64 and accompanying text.

the need to advance, develop, and promote norms to achieve those goals.[73] Under the auspices of the Shanghai Cooperation Organization, China and Russia have endorsed cybernorms as a vehicle for promoting "information security."[74] As part of the 2015 Hague Conference on Cybersecurity, both the Australian and Dutch foreign ministers added their voices to the call for cybernorms.[75] Industry actors, most notably Microsoft,[76] have advocated for new cybernorms, as have various think tanks and academic institutions.[77]

Many of the current calls for cybernorms emphasize them as an alternative to using international law (and treaties, in particular) to deal with cyber insecurity.[78] Doubts about the efficacy of treaties in this area have become widespread. Russia's initial proposals for an "information weapons" arms control treaty received a cool reception from Western states, concerned that it would not work and would also potentially be used as a justification for limiting political speech.[79] Later, Russia and other states, including China, balked at expanding membership in the Budapest Convention, deeming its cooperation requirements as too intrusive on state sovereignty.[80] The idea of using the International Telecommunication Union's Revised Radio Regulations (a treaty, despite its name) to assume Internet governance responsibilities severely

[73] WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 10 (May 2011), *at* https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; *see also* Sean Lyngaas, *NSA's Rogers Makes the Case for Cyber Norms*, FCW (Feb. 23, 2015), *at* https://fcw.com/articles/2015/02/23/nsa-rogers-cyber-norms.aspx; Sean Lyngaas, *State Department Presents Cyber Norms to Congress*, FCW (May 18, 2015), *at* https://fcw.com/articles/2015/05/18/state-cyber-norms.aspx; Catherine Lotrionte, *A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence*, GEO. J. INT'L AFF. 71, 73 (2013); Panayotis A. Yannakogeorgos & Adam Lowther, *The Prospects for Cyber Deterrence: American Sponsorship of Global Norms*, *in* CONFLICT AND COOPERATION IN CYBERSPACE, *supra* note 8.

[74] International Code of Conduct for Information Security, *in* Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, UN Doc. A/66/359, annex (Sept. 14, 2011). The Shanghai Cooperation Organization member states subsequently offered a revised version. Revised SCO Code of Conduct, *supra* note 11.

[75] *See* Julie Bishop's Statement for Plenary Session on International Peace and Security, Global Conference on Cyberspace (Apr. 17, 2015), *at* http://foreignminister.gov.au/speeches/Pages/default.aspx; Bert Koenders, Opening Speech, Global Conference on CyberSpace 2015 (Apr. 16, 2015), *at* https://www.gccs2015.com/documents.

[76] *See Five Principles for Shaping Cybersecurity Norms*, *supra* note 14, at 5–10; Paul Nicholas, *Proposed Cybersecurity Norms to Reduce Conflict in an Internet-Dependent World*, MICROSOFT: CYBER TRUST BLOG (Dec. 3, 2014), *at* https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/.

[77] *See*, *e.g.*, A CALL TO CYBER NORMS: DISCUSSIONS AT THE HARVARD–MIT–UNIVERSITY OF TORONTO CYBER NORMS WORKSHOPS, 2011 AND 2012 (2015); INTERNATIONAL CYBER NORMS, *supra* note 16; DENNIS BROEDERS, THE PUBLIC CORE OF THE INTERNET: AN INTERNATIONAL AGENDA FOR INTERNET GOVERNANCE 2 (2014), *at* http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf; Carnegie Endowment for International Peace, *Cyber Policy Initiative* (2016), *at* http://carnegieendowment.org/specialprojects/Cyber/.

[78] *See*, *e.g.*, Eichensehr, *supra* note 14, at 361–64. Alternatively, this treaty hostility might be part of a larger trend. *See* Agora, *The End of Treaties*, AJIL UNBOUND (May 2014).

[79] *See* GA Res. 53/70 (Jan. 4, 1999); Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of Information Security, UN Doc. A/54/213 (Aug. 10, 1999); Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation Addressed to the Secretary-General, UN Doc. A/C.1/53/3 (Sept. 30, 1998); Tim Maurer, *Cyber Norm Emergence at the United Nations—an Analysis of the UN's Activities Regarding Cyber-security* 17 (Belfer Center for Science and International Affairs Discussion Paper 2011-11, 2011), *at* http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

[80] *See* Budapest Convention, *supra* note 11; Alex Grigsby, *Coming Soon: Another Country to Ratify the Budapest Convention*, COUNCIL ON FOREIGN RELATIONS: NET POLITICS (Dec. 11, 2014), *at* http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/.

divided ITU member states, with dozens of states refusing to consent to the new treaty.[81] Concerns over locking in undesirable substantive or governance outcomes led the U.S. Department of State cyber coordinator, Chris Painter, to sum up the present position in Tolkienian terms, saying: "We don't need a new treaty," and "We don't need one ring to rule them all."[82] Instead, the U.S. government, like many other actors, has prioritized the creation of norms that may offer a more nimble and flexible reduce threats in the cyber environment.[83]

Despite their newfound popularity, the discourse about cybernorms is sorely underdeveloped in at least four respects. First, the norm concept is not well understood, either in terms of its constituent elements or its relationship to other concepts like law. Second, those calling for cybernorms have largely focused on the desired *products*—the particular behaviors that any new cybernorms may mandate. Efforts like the GGE's pronouncement of "peacetime" norms for state cyber-operations and the *Tallinn Manual*'s delimitation of international law norms for cyberwar focus on what norms ought to say, as if dictating the contours of a norm makes it a reality.[84] But norms form and spread in ways often not intended or foreseen by their initial promoters. Thus, it is not enough to know what cybernorms we want; we must know more about the *processes* for cultivating them.

Third, cybernorm proponents have given short shrift to the dynamic quality of norms. Norms are not locked-in agreements establishing fixed expectations; a cybernorm's meaning can (and will) evolve over time as actors interpret and apply it in different circumstances.

Fourth, and finally, by attempting to isolate particular norm candidates, states and stakeholders rarely acknowledge the pluralistic and interdependent character of cybernorms. The result is often that multiple norms arise from multiple processes covering various actors without any obvious solution to issues of overlap, competition, or conflict. In the sections that follow, we examine each of these issues and their importance for constructing cybernorms.

Norms and How They Work for Cybersecurity

Unlike *cybersecurity*, the concept of a norm is well defined in sociology and political science. According to Katzenstein's now standard definition, a norm defines "collective expectations for the proper behavior of actors with a given identity."[85] Unpacking this definition, four ingredients appear essential to the existence of a norm: (1) identity, (2) behavior, (3) propriety, and

[81] *See* International Telecommunications Union, Final Acts of the World Conference on International Telecommunications, Dubai, Dec. 3–14, 2012, *at* http://www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf; TIM MAURER & ROBERT MORGUS, TIPPING THE SCALE: AN ANALYSIS OF GLOBAL SWING STATES IN THE INTERNET GOVERNANCE DEBATE 2–3 (2014), *at* https://www.cigionline.org/sites/default/files/no7_2.pdf; Alexander Klimburg, *Commentary: The Internet Yalta* 3 (Feb. 5, 2013), *at* http://www.cnas.org/files/documents/publications/CNAS_WCIT_commentary.pdf.

[82] Brendan Nicholson, *Bishop: We Don't Support a New Cyber Crime Treaty*, AUSTRALIAN (Apr. 17, 2015), *at* http://www.theaustralian.com.au/national-affairs/foreign-affairs/bishop-we-dont-support-a-new-cyber-crime-treaty/news-story/75faf78acce6951e0d6ef35241066689.

[83] *See supra* note 73; White House, *Foreign Policy: Cybersecurity*, *at* https://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

[84] *See* 2015 GGE Report, *supra* note 9, para. 13; TALLINN MANUAL, *supra* note 11.

[85] Peter J. Katzenstein, *Introduction: Alternative Perspectives on National Security*, *in* THE CULTURE OF NATIONAL SECURITY: NORMS AND IDENTITY IN WORLD POLITICS 1, 5 (Peter J. Katzenstein ed., 1996). The older, international regimes literature defined norms as "standards of behavior defined in terms of rights and obligations." Stephen D. Krasner, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, *in* INTERNATIONAL REGIMES 1, 2 (Stephen D. Krasner ed., 1983). This definition was not well connected to the

(4) collective expectations. We can see each of these elements at work in the diversity of norms now shaping activity in cyberspace.

Identity refers to the group to which the norm applies. Norms make behavioral claims on specified types of actors, whether individuals (such as U.S. citizens, lawyers, or software developers) or larger, socially constructed groups (such as banks or states). Whatever the grouping, actors must identify themselves with that type of community for the norm to create effects. Cybernorms can potentially apply to many different identities or groups, with nation-states being the most obvious. The GGE and the Shanghai Cooperation Organization have proffered norms for *all* states,[86] but more selective groupings of states may also coalesce around norms. These may be regional groupings like the European Union and its Directive on Data Protection or the African Union's nascent efforts to regulate its member states' cybersecurity.[87] Or groupings may comprise "like-minded" states, such as the cybersecurity principles articulated for members of the North Atlantic Treaty Organization.[88] Norms may even arise for bilateral pairings of states, as witnessed by China's recent agreement on a norm against cyberespionage for commercial purposes with the United States (and, later, with the United Kingdom).[89] Given Anne-Marie Slaughter's theories on transnational government networks,[90] it is not surprising to see norms emerging for specific types of government actors, whether militaries (for example, the *Tallinn Manual*) or law enforcement communities (for example, the Budapest Convention).[91]

Cybernorms may apply to dozens of identities other than states. The Budapest Convention criminalizes (that is, delineates as improper) behavior for individuals in addition to its norms for law enforcement cooperation.[92] Various industries have norms for their members. Examples include norms for Internet service providers, hardware manufacturers, software developers, and, more generally, "critical infrastructure" industries.[93] And some groups exist for the

sociological literature, however, and ignores identity issues and vast swathes of normativity beyond "rights and obligations" that have proven central to more recent norms research.

[86] *See* 2015 GGE Report, *supra* note 9; Revised SCO Code of Conduct, *supra* note 11. The Shanghai Cooperation Organization's efforts, in particular, have proven controversial for many states, making their norm products as much an example of a like-minded grouping as of a universal one.

[87] European Commission Press Release, *supra* note 13 (re: Data Protection Directive). In 2014, the African Union adopted a cybersecurity treaty that requires fifteen ratifications to enter into force. African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, AU Doc. EX.CL/846(XXV).

[88] North Atlantic Treaty Organization, *Cyber Defence* (June 23, 2016), *at* http://www.nato.int/cps/en/natohq/topics_78170.htm.

[89] *See* White House Press Release, Fact Sheet: President Xi Jinping's State Visit to the United States, *supra* note 12; Rowena Mason, *Xi Jinping State Visit: UK and China Sign Cybersecurity Pact*, GUARDIAN (Oct. 21, 2105), *at* http://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron; *see generally* Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L & COM. REG. 443 (2015). For a discussion of norms as a "bilaterally-focused activity," see Melissa E. Hathaway & Alexander Klimburg, *Preliminary Considerations: On National Cyber Security, in* NATIONAL CYBER SECURITY FRAMEWORK MANUAL 33–34 (Alexander Klimburg ed., 2012), *at* https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

[90] ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER (2004) (see pp. 1–35 for an overview of the argument). On the relative effectiveness of transnational network communities, see Pierre-Hugues Verdier, *Transnational Regulatory Networks and Their Limits,* 34 YALE J. INT'L L. 113, 130–63 (2009).

[91] *See* TALLINN MANUAL, *supra* note 11; Budapest Convention, *supra* note 11.

[92] Budapest Convention, *supra* note 11, Arts. 2–12.

[93] The National Institute of Standards and Technology, for example, has a "Voluntary Framework" for critical infrastructure cybersecurity. *Cybersecurity Framework: Background: Framework for Improving Critical Infrastructure*

explicit purpose of promoting cybersecurity and associated norms, such as computer security incident response teams (CSIRTs), or, less happily, of destabilizing both cybersecurity and its norms.[94] Like them or not, the hacktivist group Anonymous coheres around a set of normative expectations and goals.[95] Even victims of cyberattacks may form a "group" or "identity" for the purpose of establishing cybernorms that delineate expected defensive behaviors or require disclosures of breaches, as the U.S. Securities and Exchange Commission now does for publicly traded companies.[96] Perhaps most ambitious are normative efforts to unite all "users" under the banner of multistakeholderism, as was seen at the 2014 NETmundial meeting and in its subsequent statement.[97]

Behavior refers to the specific actions required by the norm of the community. Some norms are regulative in character, creating duties or obligations that prescribe, prohibit, or permit some activity (or inactivity). Others are generative or constitutive: they create new rights or even new actors.[98] Regulatory cybernorms are already extensive in cyberspace, whether as prohibitions on behavior such as cybercrime or the use of force in cyberspace; duties such as requiring assistance to victims of severe cyberthreats; or permissions such as the use of TCP/IP.[99] Generative or constitutive norms create new actors like "systems administrator" and new institutions like the Internet Corporation for Assigned Names and Numbers (ICANN) and whatever the ongoing Internet Assigned Numbers Authority (IANA) transition may generate.[100]

For both regulative and constitutive norms, the behavioral element may vary in specificity or "depth." The legal distinctions between rules, standards, and principles provide a useful lens

Cybersecurity, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (June 9, 2016), *at* http://www.nist.gov/cyberframework/.

[94] The Forum of Incident Response and Security Teams, or FIRST, is an association of computer security incident response teams (CSIRTs) that, inter alia, offers members a "Best Practice Guide Library." *FIRST Best Practice Guide Library*, FIRST (2016), *at* https://www.first.org/resources/guides.

[95] *See* David Kushner, *The Masked Avengers: How Anonymous Incited Online Vigilantism from Tunisia to Ferguson*, NEW YORKER, Sept. 8, 2014, at 48, 50–59.

[96] U.S. Securities and Exchange Commission, *CF Disclosure Guidance: Topic No. 2: Cybersecurity* (Oct. 13, 2011), *at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[97] *NETmundial Multistakeholder Statement*, *supra* note 17, pt. 1. For an alternative survey of cybersecurity processes, see Joe Nye's "regime complexes" approach. Joseph S. Nye Jr., *The Regime Complex for Managing Global Cyber Activities* 7–13 (May 20, 2014), *at* https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities.

[98] MICHAEL BARNETT & MARTHA FINNEMORE, RULES FOR THE WORLD: INTERNATIONAL ORGANIZATIONS IN GLOBAL POLITICS 18 (2004); Michael N. Barnett & Martha Finnemore, *The Politics, Power, and Pathologies of International Organizations*, 53 INT'L ORG. 699, 710–15 (1999); Ronald L. Jepperson, Alexander Wendt & Peter J. Katzenstein, *Norms, Identity, and Culture in National Security*, *in* THE CULTURE OF NATIONAL SECURITY: NORMS AND IDENTITY IN WORLD POLITICS, *supra* note 85, at 33, 54.

[99] The Transmission Control Protocol/Internet Protocol (TCP/IP) refers to the protocols permitting end-to-end connectivity for users following a set of norms on addressing, transmitting, routing, and receiving data packets. No one is required, however, to use TCP/IP; its use is voluntary for those seeking to join the Internet. *See* 2 W. RICHARD STEVENS, TCP/IP ILLUSTRATED: THE PROTOCOLS 1–20 (1994).

[100] For decades, the Department of Commerce stewarded the authoritative root zone file, which contains names and addresses for top-level domains—.com, .org, and so on—via contracts with ICANN to carry out the Internet Assigned Numbers Authority and Verisign for root zone management. On March 14, 2014, the United States indicated it would transition authority over the Internet Assigned Numbers Authority to a new, multistakeholder process, which remains under negotiation. *See NTIA IANA Functions' Stewardship Transition*, *at* https://www.icann.org/stewardship; MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 156–84 (2002).

for understanding this sort of variation.[101] Rules involve behavioral expectations to respond *ex ante* in specific, determinate ways when certain facts exist; once the facts are clear, so, too, is the expected behavior. Specific "rules" are not hard to find in cyberspace, such as the one directing programmers to code HTML using Unicode character sets because they include every written language—in lieu of the older, English-only character-encoding scheme, ASCII.[102] By contrast, standards involve evaluation of behavior *ex post* in light of all the facts or some background policy. The U.S. Federal Trade Commission, for example, recently adopted a standard-based approach in directing companies holding third-party data to have "reasonable" cybersecurity.[103] Finally, principles set forth broad considerations for evaluating future behavior without providing any particular norm for the behavior itself. Principles can have significant weight, but they are not outcome determinative. Perhaps the most well-known principle for ICTs is the one of end-to-end design.[104]

Propriety refers to the basis on which norms label behavior as appropriate or inappropriate. The propriety of norms can have multiple bases, including religion, politics, professional standards, culture, and, importantly, law.

To date, cybernorms discourse has often focused on promoting "voluntary, nonbinding" norms as an *alternative* to law and the negotiation of a new global cybersecurity treaty.[105] But law and norms are not opposed concepts; they are intimately intertwined. One goal of those who make law (or conclude treaties) is to establish norms. The legitimacy of law (with or without a threat of sanctions) by its nature creates collective expectations of proper behavior that should, in theory, help to channel or pull the behavior of those who identify as its subjects toward conformity with its contents.[106] As Lawrence Lessig noted, law can create, displace, or change the social meaning of norms.[107] The law of treaties encapsulates this compliance pull in its fundamental norm of *pacta sunt servanda*: "Every treaty in force is binding upon the parties to it and must be performed by them in good faith."[108] Conversely, those who promote norms often view their instantiation in treaties as an important goal. As a basis for propriety,

[101] *See*, *e.g.*, Daniel Bodansky, *Rules vs. Standards in International Environmental Law*, 98 ASIL PROC. 275, 276–80 (2004); Kathleen M. Sullivan, *Foreword: The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 57–59 (1992); Pierre J. Schlag, *Rules and Standards*, 33 UCLA L. REV. 379, 381–90 (1985). Although scholarship usually focuses on the rules/standards or rules/principles distinctions, we regard all three regulatory forms as related.

[102] *See Choosing & Applying a Character Encoding*, W3C (Mar. 31, 2014), *at* https://www.w3.org/International/questions/qa-choosing-encodings (directing use of Unicode).

[103] *See* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 240–41 (3d Cir. 2015). Later, Wyndham settled with the Federal Trade Commission, agreeing to establish a consumer data-protection program. *See* Lesley Fair, *Wyndham's Settlement with the FTC: What It Means for Businesses—and Consumers*, FEDERAL TRADE COMMISSION (Dec. 9, 2015), *at* https://www.ftc.gov/news-events/blogs/business-blog/2015/12/wyndhams-settlement-ftc-what-it-means-businesses-consumers.

[104] This principle directs that, when coding, application-specific functions should occur in end hosts of networks rather than intermediary nodes. Jerome H. Saltzer, David P. Reed & David D. Clark, *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS 277, 278–80 (1984).

[105] *See*, *e.g.*, 2015 GGE Report, *supra* note 9, para. 9; *supra* notes 82–83 and accompanying text.

[106] *See generally* ABRAM CHAYES & ANTONIA CHAYES, THE NEW SOVEREIGNTY: COMPLIANCE WITH INTERNATIONAL REGULATORY AGREEMENTS (1995).

[107] Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943, 1008–16 (1995); *see also* Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338 (1997).

[108] Vienna Convention on the Law of Treaties, Art. 26, May 23, 1969, 1155 UNTS 331.

treaties have a long history of legitimacy and stability that enhances the credibility of the expectations that they define. Hence, when activists sought a global norm against the use of antipersonnel land mines, they favored the treaty vehicle for that purpose.[109] Simply put, laws can serve as a basis for formulating norms, just as norms can be codified in law.

Thus, when it comes to delineating proper from improper behavior in cyberspace, law plays an obvious role and is deeply intertwined with many norms. Every state now has domestic laws that specify appropriate behavior vis-à-vis cybersecurity or that designate other behavior as improper (for example, cybercrimes or unauthorized government operations).[110] International law also serves as a basis for cybernorms, whether those codified in the *Tallinn Manual* or recent UN affirmations of an international human right to privacy online.[111] Not all laws, of course, will form a basis for cybernorms—for example, sociologists have shown that whatever laws may say on issues of intellectual property rights, most users do not share the expectations that they set.[112]

Many (if not most) cybernorms depend, however, on bases other than law for their propriety. Among states, various political agreements offer a basis for cybernorms, such as the G-20's recent endorsement of a prohibition on cyberespionage for commercial purposes, the Organization for Security and Co-operation in Europe's Parliamentary Declaration & Resolution on Cybersecurity, and the Shanghai Cooperation Organization's Code of Conduct for Information Security.[113] Multistakeholder processes like NETmundial (which involved NGOs, firms, and individuals) or the Montevideo Statement (which was signed by the major Internet institutions) suggest that the political basis of propriety can also arise among actors other than states.[114]

The propriety of cybernorms—the "oughtness" of their normative claims—can have sources beyond law and politics, most notably in culture.[115] Several distinct cultures converge in cyberspace, creating an array of normative claims. The culture of Silicon Valley—with its emphasis on security and privacy—accounts for much of the current resistance to back or front doors in software by companies like Apple, and contrasts with the cultural expectations of those

[109] *See* Kenneth Anderson, *The Ottawa Convention Banning Landmines, the Role of International Non-governmental Organizations and the Idea of International Civil Society*, 11 EUR. J. INT'L L. 91, 104–09 (2000); Stuart Maslen & Peter Herby, *An International Ban on Anti-personnel Mines: History and Negotiation of the "Ottawa Treaty,"* 38 INT'L REV. RED CROSS 693 (1998).

[110] *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C.A. §1030 (2012) (United States); Computer Misuse Act 1990, ch. 18, §§5(2)(b), (3)(b) (United Kingdom); Criminal Law of the People's Republic of China, Art. 286 (Mar. 14, 1997) (China); Penal Code §202a(1) (Germany); Information Technology Act 2008 §43(a) (India).

[111] TALLINN MANUAL, *supra* note 11; Information and Communications Technology for Development, GA Res. 68/198 (Dec. 20, 2013).

[112] Måns Svensson & Stefan Larsson, *Intellectual Property Law Compliance in Europe: Illegal File Sharing and the Role of Social Norms*, 14 NEW MEDIA & SOC. 1147, 1157–60 (2012).

[113] *See G-20 Leaders' Communiqué, Antalya Summit, November 15–16, 2015*, para. 26, *at* http://www.mofa.go.jp/files/000111117.pdf; Organization for Security & Co-operation in Europe, 2013 Istanbul Final Declaration and Resolution on Cyber Security, *at* https://www.oscepa.org/meetings/annual-sessions/2013-istanbul-annual-session/2013-istanbul-final-declaration/1652-15; Revised SCO Code of Conduct, *supra* note 11.

[114] *NETmundial Multistakeholder Statement*, *supra* note 17; *Montevideo Statement on the Future of Internet Cooperation*, ICAAN (Oct. 7, 2013), *at* https://www.icann.org/news/announcement-2013-10-07-en.

[115] Katzenstein, *supra* note 85, at 6 ("Culture refers to both a set of evaluative standards (such as norms and values) and a set of cognitive standards (such as rules and models) that define what social actors exist in a system, how they operate, and how they relate to one another.").

working in national security and law enforcement who are seeking exactly that sort of access.[116] Professional norms—the culture associated with a particular profession—also play a key role in contemporary cybersecurity. The behavior of chief information security officers owes much to the rules and professional standards associated with the culture within which they were trained and now operate.[117]

Finally, *collective expectations* refer to the social and intersubjective character of norms. Norms are not unilateral edicts but shared understandings about appropriate behavior held by members of the designated group. Norms are what social scientists call *social constructions*. They exist only because we all believe they exist. Money is a social construction. The paper in your wallet has value only because the people around you all believe it has value. Intersubjectivity—the shared belief in the paper's characteristics—is what allows you to get a coffee in exchange for paper. The paper, as material object, has little value. Similarly, norms exist and are "real" only because we all share the expectation that their behavioral claims are widely understood. We queue for movie tickets and receive visiting heads of state on red carpets because these behaviors are expected; we may not even consciously consider alternative behaviors—and if we did, we know there would be social costs.

The extent of this intersubjectivity can (and does) vary for different norms. In the cyber context, the propriety of using cyberspace for commercial purposes, which at one time was questioned, has become so ingrained that few, if any, question it any more.[118] Other norms, by contrast, remain actively contested, such as the propriety of coding with encryption or allowing victims of hacking to engage in active defense (that is, hacking back).[119] In between these two poles, collective expectations can involve more intermediate forms. One such form involves norms that receive only *insincere conformity*; that is, some (or all) members of the group give lip service to the norm but resist any change in their behavior. Cybersecurity experts are currently debating whether China's commitment to forgo cyberespionage for commercial advantage is one such norm.[120] Even if the commitment to this norm was insincere, however, it would be a mistake to dismiss it entirely. As the history of the Helsinki Accords shows, original insincerity (in that case Soviet insincerity about human rights obligations) may evolve over time toward compliance through a variety of processes.[121] Actors may need to correct the cognitive dissonance (or charges of hypocrisy) that accompany a misalignment of actions

[116] *See supra* notes 1–5 and accompanying text.

[117] *See, e.g.*, CISO Executive Forum, INFORMATION SYSTEMS SECURITY ASSOCIATION (2016), *at* https://www.issa.org/?page=CISOhome.

[118] *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 190 (1999); Shane Greenstein, *Commercialization of the Internet: The Interaction of Public Policy and Private Choices or Why Introducing the Market Worked So Well*, in 1 INNOVATION POLICY AND THE ECONOMY 151, 154 (Adam B. Jaffe, Josh Lerner & Scott Stern eds., 2001), *at* http://www.nber.org/chapters/c10779.pdf.

[119] *See supra* notes 1–5, 15, 116, and accompanying text (re: encryption); Stewart Baker, *Making Hackback Humdrum*, WASH. POST: VOLOKH CONSPIRACY (Nov. 22, 2015), *at* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/22/making-hackback-humdrum/; Patrick Lin & Heather Roff, *Should Washington Allow Companies to Strike Back Against Hackers?* WALL ST. J., May 10, 2015, at R5.

[120] *Compare* Emilio Iasiello, *Ramping Down Chinese Commercial Cyber Espionage*, FOREIGN POL'Y J. (Dec. 9, 2015), *at* http://www.foreignpolicyjournal.com/2015/12/09/ramping-down-chinese-cyber-espionage/, *with* Franz-Stefan Gady, *Top US Spy Chief: China Still Successful in Cyber Espionage Against US*, DIPLOMAT (Feb. 16, 2016), *at* http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us/.

[121] The Helsinki Accords set up an organizational forum—which today has become the Organization for Security and Co-operation in Europe—to host dialogues on issues ranging from human rights to security. *See*

and words. Lip service and formal adherence may also provide a platform for those pressuring for change, as it did when the group Helsinki Watch—later Human Rights Watch—was created.[122]

Another intermediate form of collective expectations reflects what Cass Sunstein described as *incompletely theorized agreements*.[123] In those situations, members of the group share an expectation of what constitutes proper behavior without agreement on *why* the behavior is proper. Sunstein uses religious liberty as an example: everyone may believe in it, but for vastly different reasons. Some favor religious freedom to preserve their own beliefs; some view it as a moral command; some accept its existence on utilitarian grounds; and others may see it as a matter of national security—a way to preserve social peace.[124]

Cyberspace appears to include norms that are "incompletely theorized" in Sunstein's sense. Consider the norm that ICT creators, operators, and users should responsibly disclose ICT vulnerabilities. Although the norm has been widely adopted, actors differ dramatically in *why* they adopt the norm. For ICT companies, disclosure and also patching have an economic motivation—namely, to preserve their company's bottom line. Some researchers who seek bounty payments for finding such vulnerabilities are similarly motivated, whereas others believe responsible disclosure is a social responsibility. States, meanwhile, may expect responsible disclosure for national security reasons: to ensure the confidentiality and integrity of the ICT they use. And users may favor the norm because it aligns with their privacy interests.[125]

Thus, cyberspace is not a norm vacuum—far from it. We already have a wide variety of norms governing diverse aspects of ICTs. These extant norms vary widely on all definitional dimensions. They apply to diverse types of actors having different identities. They make diverse claims on behavior; sometimes *pre*scribing, other times *pro*scribing action. Norms may also *generate* or *constitute* new actors, social facts, and organizational structures. They can vary in their degree of internalization and draw their propriety or normative force from a wide variety of contexts and cultures, including (but not limited to) law. Like the varying contexts implicating cybersecurity, efforts to construct new cybernorms must account for this normative heterogeneity. At the same time, however, to be successful such efforts must also understand the *processes* by which norms arise and shape behavior in the first place.

Conference on Security and Co-operation in Europe: Final Act, 14 ILM 1292 (1975), *available at* http://www.osce.org/helsinki-final-act?download=true.

[122] *See generally* DANIEL C. THOMAS, THE HELSINKI EFFECT: INTERNATIONAL NORMS, HUMAN RIGHTS, AND THE DEMISE OF COMMUNISM (2001). Risse, Ropp, and Sikkink's "spiral model" of human rights change provides a more detailed theorization of this process. *See* Thomas Risse & Kathryn Sikkink, *The Socialization of International Human Rights Norms into Domestic Practices: Introduction*, *in* THE POWER OF HUMAN RIGHTS: INTERNATIONAL NORMS AND DOMESTIC CHANGE 1, 17–35 (Thomas Risse, Stephen C. Ropp & Kathryn Sikkink eds., 1999).

[123] Cass R. Sunstein, *Incompletely Theorized Agreements in Constitutional Law*, 74 SOC. RES. 1 (2007). Sunstein's idea shares some similarities with John Rawls's ideas of overlapping consensus. *See* John Rawls, *The Idea of an Overlapping Consensus*, 7 OXFORD J. LEGAL STUD. 1 (1987).

[124] Sunstein, *supra* note 123, at 1–3.

[125] *See* Ryan Ellis, *The Vulnerability Economy: Zero-Days, Cybersecurity, and Public Policy* 3–6 (Feb. 4, 2015), *at* https://cb.hbsp.harvard.edu/cbmp/product/KS1013-PDF-ENG; *Vulnerability Disclosure Policy* (2016), CERT, *at* http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm.

A Process-Oriented View of Norms

Norms arise in many ways. They may emerge spontaneously or through the entrepreneurship of one or more actors who frame the issue, articulate the norm, and organize support. If such efforts are successful, the norm may reach a tipping point and cause a "cascade" of norm adoption or, in other cases, cycles of norm change. Norm promoters draw on a variety of tools to construct the norm and create support for it, including incentives, persuasion, and socialization.

Norm catalysts: Habit or entrepreneurship? Some norms emerge spontaneously, without any particular intent by any particular actor.[126] In any social setting where actors interact regularly, norms will develop simply through repeated behavior since such behavior creates expectations in others. Consider a group walking into a conference room for a week of meetings. On the first day, people may sit more or less randomly around the table, particularly if they do not know each other and there are no obvious hierarchies. On subsequent days, though, people tend to sit where they sat before. By the end of the week, actors think of the seats as "Jane's seat" or "Joe's seat." Habit and repetition alone—particularly when they go unchallenged—create norms.

This power of past behavior to shape present expectations is well known and widely studied across the social sciences. Much has been written now about path dependence, whereby decisions in the past constrain options in the present or future regardless of their continued efficiency. In the history of technology, path dependence often looms large, the QWERTY keyboard design being the archetypical example.[127] The idea is also familiar to international lawyers. Among their sources, international legal norms may emerge from custom—a practice that states generally follow in a sufficiently uniform way over time such that eventually those same states accept it as law.[128] The history of the Internet is rife with examples of cybernorms that appeared out of habit. The widespread preference for using Simple Network Management Protocol (SNMP) to manage devices on a network emerged from its repeated use, notwithstanding the availability of other protocols that performed the same function with fewer security vulnerabilities.[129]

States are very much aware of the power of unchallenged repetition to create new norms. The U.S. indictment in May 2014 of five members of the Chinese People's Liberation Army, who were accused of hacking into the networks of U.S. corporations, was clearly aimed at disrupting momentum for developing a norm that permitted state-sponsored cyberespionage for commercial advantage. With public release of the indictments, the United States aimed to derail

[126] *See* Robert Sugden, *Spontaneous Order*, 3 J. ECON. PERSP. 85, 87–97 (1989).

[127] *See* Paul A. David, *Clio and the Economics of QWERTY*, 75 AM. ECON. REV. 332 (1985). The QWERTY configuration on contemporary keyboards was designed for inefficiency—to slow typists and keep manual keys from jamming. Today, we remain locked into this suboptimal social norm for keyboard construction because switching to a more efficient alternative is too costly. *Id.* at 333–36.

[128] When and how to distinguish mere repeated practices of states from those accepted as law remains subject to debate. *See*, *e.g.*, Jörg Kammerhofer, *Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems*, 15 EUR. J. INT'L L. 523, 525–26 (2004); Anthea Elizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 AJIL 757, 757–60 (2001).

[129] *See* Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts & Stephen Wolff, *A Brief History of the Internet* 13 (2003), *at* http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf.

normalization of this kind of espionage and to delegitimate it.[130] For its part, and before agreeing to denounce the practice in September 2015, China rejected the U.S. charges and used the Snowden leaks to call attention to instances of U.S. cyberespionage against Chinese companies, such as Huawei.[131]

U.S. coyness about authorship of the Stuxnet attack on Iranian centrifuges may have a similar logic.[132] The reluctance of the United States and other states to take credit for the attack or even discuss their offensive cyber capabilities stems in part from fear of setting precedents and "normalizing" similar cyberattacks to which the United States itself might be particularly vulnerable. The same pattern of behavior was on display over U.S. cyber-exploitations, even as Edward Snowden revealed their full scope.

Many—probably most—of the norms that we care about for regulatory purposes, however, do not arise spontaneously. They are the product of hard work by interested parties who are often called *norm entrepreneurs*.[133] These entrepreneurs may be any actor or actors who have a norm that they want to promote, whether for groups of which they are members or for some other community to adopt. Norm entrepreneurs may be individuals, like Henry Dunant, founder of the International Committee of the Red Cross, who, in 1863, first proposed the norms now at the core of the Geneva Conventions.[134] They may be NGOs like Transparency International that define and promote new norms against corruption,[135] or they may be coalitions of NGOs and other actors like the International Campaign to Ban Landmines.[136] Firms, of course, may also promote norms; as already noted, Microsoft is playing such a role currently in the push for global norms for cybersecurity. International organizations like the United Nations can be norm entrepreneurs. Through its many agencies, the United Nations is proposing new norms all the time, such as the Responsibility to Protect.[137] And states, of course,

[130] U.S. Department of Justice Press Release, *U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (May 19, 2014), *at* https://www.fbi.gov/pittsburgh/press-releases/2014/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage; Michael S. Schmitt & David Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES, May 20, 2014, at A1.

[131] *See* Shannon Tiezzi, *China's Response to the US Cyber Espionage Charges*, DIPLOMAT (May 21, 2014), *at* http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges/; Marc Ferranti, *Reports: NSA Hacked into Servers at Huawei Headquarters, Reports Say*, PCWorld (Mar. 23, 2014), *at* http://www.pcworld.com/article/2110960/nsa-hacked-into-servers-at-huawei-headquarters-reports-say.html.

[132] Although the United States never formally admitted a role in Stuxnet, media reports have made that claim. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1; DEIBERT, *supra* note 23, at 177.

[133] *See*, *e.g.*, Finnemore & Sikkink, *supra* note 18, at 895–99; Stacie E. Goddard, *Brokering Change: Networks and Entrepreneurs in International Politics*, 1 INT'L THEORY 249 (2009); Amitav Acharya, *How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism*, 58 INT'L ORG 239 (2004); Harold Hongju Koh, *Why Do Nations Obey International Law,* 106 Yale L.J. 2599, 2630–34, 2648 (1997); Cass R. Sunstein, *Social Norms and Social Rules*, 96 COLUM. L. REV 903, 929 (1996).

[134] *See*, *e.g.*, MARTHA FINNEMORE, NATIONAL INTERESTS IN INTERNATIONAL SOCIETY 69–88 (1996); Kathryn Sikkink, *Transnational Politics, International Relations Theory, and Human Rights*, 31 POL. SCI. & POL. 517, 518–19 (1998).

[135] *See* Kenneth W. Abbott & Duncan Snidal, *Values and Interests: International Legalization in the Fight Against Corruption*, 31 J. LEGAL STUD. S141, S154–71 (2002); Hongying Wang & James N. Rosenau, *Transparency International and Corruption as an Issue of Global Governance*, 7 GLOBAL GOVERNANCE 25, 30–38 (2001).

[136] *See* Richard Price, *Reversing the Gun Sights: Transnational Civil Society Targets Land Mines*, 52 INT'L ORG. 613, 620–39 (1998).

[137] *See* Alex J. Bellamy, *The Responsibility to Protect—Five Years On*, 24 ETHICS & INT'L AFF. 143, 143 (2010). Before R2P garnered UN support, Gareth Evans first articulated it as chair of a Canada-sponsored international

can be norm entrepreneurs. The United States, for example, was the leading proponent of prohibiting states from engaging in cyberespionage for commercial advantage.[138]

Norm entrepreneurs are critical to norm emergence not only because they call attention to an issue but because they *frame* it—they use language that names, interprets, and dramatizes the problem—and on that basis propose a norm to address it.[139] Framing defines the problem involved in a particular way and tells us who should do what to tackle the problem so framed. Struggles over framing have significant long-term consequences since frames tend to be sticky and hard to dislodge.[140] This stickiness can create a first-mover advantage in struggles to frame new norms. Mobilizing support for one's own version of the norm before the competition does can pay dividends since latecomers need to position themselves not just as improvements on the status quo but as improvements over the first mover.

Successful (re)framing of an issue requires strategy and activism on multiple levels to succeed. For example, the International Campaign to Ban Landmines worked hard to reframe the meaning and significance of anti-personnel mines in the 1990s. They had to convince militaries and publics that a boring piece of defensive hardware was more properly understood as an egregious violation of the laws of war and human rights because those mines were indiscriminate, could not be targeted, and remained lethal years after conflicts ended. Graphic photos of harm inflicted on civilians, particularly children, and the involvement of celebrities like Princess Diana helped extend the new frame beyond a narrow legal community, giving the promotion effort broad resonance with publics and politicians. Eventually, these new frames generated state allies, notably the Canadians, as well as further NGO support that led to the Ottawa Convention.[141]

Framing efforts already feature prominently in norm proposals for cybersecurity. Consider again the push to have supply chains for software incorporate back or front doors to allow law enforcement to circumvent encryption when they have a need to do so.[142] Proponents of such a norm frame it as a necessary response to security threats—for example, child abductions and terror cell communications.[143] Opponents use different frames to challenge both the need for the norm (suggesting law enforcement can accomplish its goals without back or front doors) and its overall costs to user cybersecurity (arguing, for example, that there is no technical way

commission. INTERNATIONAL COMMISSION ON INTERVENTION AND STATE SOVEREIGNTY, THE RESPONSIBILITY TO PROTECT, at vii (2001), *at* http://responsibilitytoprotect.org/ICISS%20Report.pdf

[138] *See supra* notes 12, 130–31, and accompanying text.

[139] On frames and "frame alignment," see generally Robert D. Benford & David A. Snow, *Framing Processes and Social Movements: An Overview and Assessment*, 26 ANN. REV. SOC. 611 (2000); David A. Snow, E. Burke Rochford Jr., Steven K. Worden & Robert D. Benford, *Frame Alignment Processes, Micromobilization, and Movement Participation*, 51 AM. SOC. REV. 464 (1986).

[140] As a result, framing is a lively research topic in sociology, political science, and other fields. *See*, *e.g.*, Dennis Chong & James N. Druckman, *A Theory of Framing and Opinion Formation in Competitive Elite Environments*, 57 J. COMM. 99 (2007); Robert D. Benford, *An Insider's Critique of the Social Movement Framing Perspective*, 67 SOC. INQUIRY 409 (1997). Lessig uses the term *meaning managers* to describe this kind of agency in shaping norms and social context. Lawrence Lessig, *Social Meaning and Social Norms*, 144 U. PA. L. REV. 2181, 2189 (1996).

[141] *See generally* Price, *supra* note 136.

[142] *See supra* notes 1–3, 15, 116, and accompanying text.

[143] *See*, *e.g.*, Cyrus R. Vance Jr., François Molins, Adrian Leppard & Javier Zaragoza, *When Phone Encryption Blocks Justice*, INT'L N.Y. TIMES, Aug. 12, 2015, at 8.

to limit access to back or front doors by those intent on malicious use, with the consequence that the security of all users would be compromised).[144]

Beyond framing, norm entrepreneurs often create *organizational platforms* from which to do the difficult work of promoting and embedding their norms.[145] Some entrepreneurs may build a new organization for that express purpose, as Dunant and his colleagues built the International Committee of the Red Cross. Others may "graft" their efforts onto existing norms and organizations to facilitate institutionalization and dissemination.[146] The United States and like-minded states have used the GGE (which was originally set up at the behest of the Russian Federation) to advance their agenda for establishing various peacetime norms for states in cyberspace.[147] Anchoring the process at the United Nations has allowed for a broad-based platform and helped to legitimate the consensus documents produced.[148]

Patterns of norm adoption vary, but a common pattern is the one noted by Sunstein, among others. Entrepreneurs struggle hard to secure norm adoption in the early going. If they are skilled and lucky, they reach some critical mass or tipping point of norm adherents, and the norm cascades through the target population.[149] Predicting tipping points is tricky, and social science does not offer good guidance about forecasting when cascades will happen. Nonetheless, cascade patterns have been documented in a great many norm-promotion efforts, including adoption patterns for a variety of human rights treaties.[150] The rapid acceptance of the prohibition on cyberespionage for commercial advantage may be in the midst of an ongoing cascade, as its adherents quickly grew from the United States and China, to include the United Kingdom and eventually the whole G-20.[151]

Another interpretation of norm adoption patterns sees "cycles" rather than "cascades." Taking the long historical view, Wayne Sandholtz and others emphasize that new norms always

[144] *See* David Kaye (Special Rapporteur), Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression, paras. 13, 42, UN Doc. A/HRC/29/32 (May 22, 2015).

[145] Finnemore & Sikkink, *supra* note 18, at 896–901.

[146] *See* Acharya, *supra* note 133, at 243–45; Price, *supra* note 136, at 617.

[147] The 2015 GGE Report called on states to support various peacetime cybernorms, including the following: not conducting or knowingly supporting ICT activity that intentionally damages critical infrastructure; not knowingly targeting another state's CSIRTs; and not using their own CSIRTs for malicious activity. 2015 GGE Report, *supra* note 9, para. 13.

[148] Alex Grigsby, *The 2015 GGE Report: Breaking New Ground, Ever So Slowly*, NET POLITICS (Sept. 8, 2015), *at* http://blogs.cfr.org/cyber/2015/09/08/the-2015-gge-report-breaking-new-ground-ever-so-slowly/; Elaine Korzak, *The 2015 GGE Report: What Next for Norms in Cyberspace?*, LAWFARE (Sept. 23, 2015), *at* https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace/.

[149] CASS R. SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 38 (1999).

[150] *See* KATHRYN SIKKINK, THE JUSTICE CASCADE: HOW HUMAN RIGHTS PROSECUTIONS ARE CHANGING WORLD POLITICS 11 (2011); Udi Sommer & Victor Asal, *A Cross-national Analysis of the Guarantees of Rights*, 35 INT'L POL. SCI. REV. 463 (2014). "World polity" theorists (sometimes called "sociological institutionalists," or "the Stanford School") would argue that these cascades are part of a powerful world culture that has spread and thickened over the past century as many norms and organizational forms have "gone global." The spread of cybernorms would very much fit with their arguments. *See* GEORGE M. THOMAS, INSTITUTIONAL STRUCTURE: CONSTITUTING STATE, SOCIETY, AND THE INDIVIDUAL (1987); John Boli & George M. Thomas, *Introduction* to CONSTRUCTING WORLD CULTURE: INTERNATIONAL NONGOVERNMENTAL ORGANIZATIONS SINCE 1875, at 1 (John Boli & George M. Thomas eds., 1999); John W. Meyer, John Boli, George M. Thomas & Francisco O. Ramirez, *World Society and the Nation-State*, 103 AM. J. SOC. 144 (1997).

[151] *See supra* notes 12, 89, 113, and accompanying text.

grow out of problems with, and disputes about, existing norms.[152] Because no norm fits all contexts perfectly, and no system of rules can be complete, there will always be pressures to change old norms and create new ones. Importantly for the cyber context, these arguments emphasize the ways that norm-cultivation efforts are always shaped and constrained by existing understandings. Existing contexts, as we emphasized earlier, are what create the opportunities and tools for norm construction, and also the obstacles. Thus, efforts to elaborate norms on the use of force via cyber-operations must account for the nature and scope of existing norms on the use of force while simultaneously exploring the novel conditions that ICTs impose—conditions that are continuing to create pressure for new norms.[153]

Whatever their pattern of spread, norms on important contentious issues do not just diffuse like gasses. Cultivating norms requires serious effort.[154] Successful promoters must draw upon diverse resources in strategizing how best to accomplish their goals. Several types of tools are available for forming norms and for then spreading them within a given community.

Scholars of both international law and international relations have carefully studied mechanisms for the creation and operation of international norms. Whether emerging out of habit or entrepreneurship, there are at least three discrete tools for promoting the progressive development and spread of norms: (1) incentives, (2) persuasion, and (3) socialization.[155]

Incentives. Strong actors—in particular, strong states—often have vast resources at their disposal to propagate norms they like through incentives of various kinds. They can offer positive inducements—for example, preferential trade arrangements or weapons deals—that might incentivize others to support a state's preferred norm and comply with it.[156] Old-fashioned coercion—economic sanctions and, at the extreme, military actions or credible threats thereof—can also be deployed to promote the norms of the strong. Nor is the incentive tool limited to states or even to "strong" actors. NGOs put great effort into creating rewards and punishments for their target audiences; they may, among other things, organize protests and boycotts, and issue best/worst lists.[157] Still, strong actors do have advantages in this realm. The United

[152] *See generally* WAYNE SANDHOLTZ & KENDALL STILES, INTERNATIONAL NORMS AND CYCLES OF CHANGE (2009); WAYNE SANDHOLTZ, PROHIBITING PLUNDER: HOW NORMS CHANGE (2008).

[153] *See* TALLINN MANUAL, *supra* note 11; Duncan B. Hollis, *Re-thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, *in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS 129 (Jens Ohlin, Kevin Govern & Claire Finkelstein eds., 2015).

[154] This is true for law as well as for norms more generally. *See* JUTTA BRUNNÉE & STEPHEN J. TOOPE, LEGITIMACY AND LEGALITY IN INTERNATIONAL LAW: AN INTERACTIONAL ACCOUNT 8 (2010).

[155] These processes are deeply intertwined, and scholars employ varying nomenclature and categorizations. Goodman and Jinks focus on material inducement, persuasion, and acculturation. RYAN GOODMAN & DEREK JINKS, SOCIALIZING STATES: PROMOTING HUMAN RIGHTS THROUGH INTERNATIONAL LAW 4 (2013). Johnston condenses the mechanisms to two: persuasion and social influence. Alastair Iain Johnston, *Treating International Institutions as Social Environments*, 45 INT'L STUD. Q. 487, 487 (2001). Checkel emphasizes strategic calculations, role playing, and normative suasion. Jeffrey T. Checkel, *International Institutions and Socialization in Europe: Introduction and Framework*, 59 INT'L ORG. 801 (2005).

[156] Our analysis assumes that incentives (and persuasion and socialization) are felt by states and other institutions via human agents who represent them. There is therefore no need to anthropomorphize states in order to rely on the sociological literature to assess behavior and beliefs. *Accord* GOODMAN & JINKS, *supra* note 155, at 40–41.

[157] *See, e.g.*, *2015 Heroes and Villains of Human Rights and Communication Surveillance*, ACCESS NOW (2016), *at* https://www.accessnow.org/announcing-the-2015-heroes-villains-of-human-rights-and-communications-surveillance/. The international relations literature often focuses on nongovernmental organizations and otherwise weak actors since these norm entrepreneurs challenge various theoretical assumptions about international relations—most notably, the realist view. But we should still remain attentive to the pervasive role of the strong in creating norms.

States and its allies, for example, have not been at all shy about using threats or bribes to promote desired behavior and to shape collective expectations on issues ranging from human rights and democracy to neoliberal economic policies. The European Union provides a recent cybersecurity example via its new General Data Protection Regulation, which instantiates, in law, various new data-protection norms, with the threat of tremendous fines for companies that fail to comply with its terms.[158]

Coercive powers—bribes and threats—raise important questions not only about norm processes but about the nature of normativity itself. Does something "count" as a norm if the desired behavior is coerced (or bribed) rather than being sincerely believed or accepted? Is a norm really a norm if we do not like its contents? At one level, the answer is obviously yes. Individuals do things all the time that are not their preferred behaviors. Most of us would not choose to wear neckties or high heels, but we do so when the occasion demands it—that is, when it is "proper" and appropriate. We might do so in a conscious and calculating way (we do not want to lose our jobs, or we desire our family's support). In those cases, we would expect compliance to last only as long as the incentives persist.

In other cases, some amount of *internalization* of the norm occurs; that is, actors continue to comply even when incentives cease or are reduced. All norm entrepreneurs—from parents to states—aspire to have their norms fully internalized by the relevant community. Parents hope that their children will continue to say please and thank-you, not run with scissors, and wash their hands before meals even in the absence of parental bribes or punishments. They hope, too, that their children will become sincerely convinced of the virtue—or at least the necessity—of these behaviors.

The same logic motivates international norm entrepreneurs who seek to incentivize actors' behavior.[159] Those actors, including states, may initially adhere to norms as part of tactical bargains, perhaps cynically struck, in response to coercion or material inducements. But over time, norm compliance may become routinized as habits take hold, such that norm-conforming behavior continues without the presence of norm entrepreneurs or incentives.[160] As we noted earlier, organizational structures and bureaucratic processes may facilitate the construction of normative habits by codifying norm-compliance expectations in rules or procedures, and by incorporating norms into the technical and professional training of those doing relevant jobs.

Persuasion. Persuasion is ubiquitous in norm promotion. Following standard usage, we understand persuasion to mean causing someone to do or believe something by asking, arguing, or giving reasons. It is primarily a cognitive process of information exchange and argumentation that changes minds, opinions, and attitudes about causality and effect in the absence of coercion.[161] Disseminating new information is a key part of the persuasive process, yet new

[158] *See*, *e.g.*, European Commission Press Release, *supra* note 13; Warwick Ashford, *EU Data Protection Rules Affect Everyone, Say Legal Experts*, COMPUTERWEEKLY (Jan. 11, 2016), *at* http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts.

[159] For more on norm internalization, including the idea of "obedience," see Koh, *supra* note 133.

[160] *See supra* notes 126–32 and accompanying text (re: habit).

[161] For an interdisciplinary assessment of persuasion, see Steven R. Ratner, *Law Promotion Beyond Law Talk: The Red Cross, Persuasion, and the Laws of War*, 22 EUR. J. INT'L L. 459 (2011). Johnston and Goodman/Jinks differentiate persuasion, which is cognitive, from social influences and socialization, which are rooted in relationships. They recognize, moreover, that ideal-type distinctions break down in empirical situations since most real-world interactions involve both cognition and social relations. Johnston, *supra* note 155, at 496; GOODMAN & JINKS, *supra* note 155, at 29–30. Jürgen Habermas's work on "communicative action" is central to much persuasion

information alone is often insufficient to change minds. Facts rarely speak for themselves. They must be interpreted and contextualized to create desired effects. Several techniques exist for doing that, most notably *framing* and *linking*.

As we discussed above, the *framing* of facts and arguments matters greatly to their persuasive power.[162] In addition, *linking* one's preferred norm to other powerful norms can increase its credibility and urgency. For example, embedding norms in larger "narratives" about security or identity can enhance their persuasive power and make compliance more compelling.[163] Thus, the U.S. National Institute of Standards and Technology has promoted its "voluntary" Cybersecurity Framework by linking its adoption by critical infrastructure industries to matters of both "national and economic security."[164] Conversely, of course, norms not linked to dominant narratives like national security or identity may be neglected.

Socialization. Beyond concrete incentives or cognitive frames and linkages, social relations can also generate or disseminate norms. *Socialization* refers to processes by which newcomers become incorporated into organized patterns of social interaction.[165] It rests on social relations and the identity ingredient of the norm concept: an actor wanting to establish or maintain a relationship with another actor or group of actors will conform to a norm, not necessarily because of its content but because doing so is expected within a valued relationship. Motors for socialization are diverse and complex. Factors commonly cited in the literature include cognitive discomfort with "bucking" expectations in a valued relationship and, conversely, the comfort and self-esteem gained through conformity.[166]

Initially, socialization may take the form of *mimicry*. A state, for example, may conform its behavior to norms of one or more states that it perceives as successful, specifically on the theory that that is how successful states behave. Such mimicry can be an instrumental calculation along the lines of "to get where they are, I should do what they do," but it can equally be a more affective response such as "to be part of this group and respected by its members, I should emulate their behavior." Developing states, for example, often emulate both the behaviors and the structures of more developed states; they adopt Western-style education systems,[167] suffrage laws,[168] and perhaps now even military cyberforces.[169] For those actors that already self-identify with a given community, continued conformity with the group's norms, even as those

research. 1 JÜRGEN HABERMAS, THEORY OF COMMUNICATIVE ACTION (1984). For international relations applications, see Thomas Risse, "*Let's Argue!": Communicative Action in World Politics*, 54 INT'L ORG. 1 (2000).

[162] *See supra* notes 139–44 and accompanying text.

[163] *See generally* RONALD R. KREBS, NARRATIVE AND THE MAKING OF US NATIONAL SECURITY (2015).

[164] *See Cybersecurity Framework*, *supra* note 93.

[165] Sheldon Stryker & Anne Statham, *Symbolic Interaction and Role Theory*, *in* 1 THE HANDBOOK OF SOCIAL PSYCHOLOGY 311, 325 (Garnder Lindzey & Elliot Aronson eds., 1985) ("Socialization is the generic term used to refer to the processes by which the newcomer—the infant, rookie, or trainee, for example—becomes incorporated into organized patterns of interaction."); Johnston, *supra* note 155, at 494 (quoting Stryker & Statham, *supra*). Goodman and Jinks refer to "acculturation"—"the general process by which actors adopt the beliefs and behavioral patterns of the surrounding culture." GOODMAN & JINKS, *supra* note 155, at 4.

[166] Johnston, *supra* note 155, at 500. Socialization often has a strong status element, with lower-status actors seeking to meet expectations (and adopt the norms) of high-status actors. *Id.*

[167] *See* John W. Meyer, Francisco O. Ramirez & Yasemin Nuhoglu Soysal, *World Expansion of Mass Education, 1870–1980*, 65 SOC. EDUC. 128 (1992).

[168] Francisco O. Ramirez, Yasemin Soysal & Suzanne Shanahan, *The Changing Logic of Political Citizenship: Cross-national Acquisition of Women's Suffrage Rights, 1890 to 1990*, 62 AM. SOC. REV. 735 (1997).

[169] *See supra* note 66 and accompanying text. For more on mimicry, see Paul DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147, 151 (1983).

norms change, may be a purposeful or an automatic response to maintain or maximize their status within the given community.

Norm promoters are aware of these processes and harness them to bring noncomplying actors to accept their preferred norms. They have a variety of tools available for that purpose. Norm promoters can exploit the extent to which states and other actors are concerned with their reputations within a specific community. For example, if norm conformance is seen as something that enhances national prestige, promoters can use that to their advantage. Framing a norm as a "best practice" and securing early adoption by a few key high-status or successful actors can induce mimicry and conformity in others. Norm promoters can assist this process by providing help to novice adopters as they endeavor to conform to new norms and "do the right thing." "Technical assistance" of many kinds is designed and offered with this goal in mind. In cybersecurity, the CERT Coordination Center of the Software Engineering Institute at Carnegie Mellon University, among others, provides assistance to countries to set up and operate computer security incident response teams on the theory that all states (and other interested actors) should have one.[170]

Professional training is yet another tool of socialization. Embedding norms in curricula, duties, and standards for good professional conduct can be a powerful way to ensure values embedded in the norm are inculcated into key actors in organizations and also into the policies that they implement. An example from cybersecurity involves the U.S. Telecommunications Training Institute, which offers training to regulators, professionals, and entrepreneurs from the developing world.[171]

Socialization mechanisms are not all "carrots"; some are sticks and can be coercive. Norm promoters may try to label nonconformers as "rogues" who are not to be trusted, thereby threatening their status and their reputations. "Naming and shaming" of norm violators is a well-known tool of activists seeking to promote norms—one available even to weak actors seeking to change behavior of much more powerful parties like states or big multinational firms.[172] Publicizing names of norm violators can inflict reputational costs and compromise the credibility of violators in ways that are in some sense coercive, but any behavioral changes are actually achieved through speech and social relations rather than material incentives. Similarly, actors can become "entrapped" by prior rhetorical commitments in ways that nudge them toward norm conformity and, sometimes, sincere acceptance.[173] Entrapment creates the

[170] *Create a CSIRT*, CERT (2016), *at* http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm; Robert Morgus, Isabel Skierka, Mirko Hohmann & Tim Maurer, *National CSIRTs and Their Role in Computer Security Incident Response*, NEW AMERICA (Nov. 19, 2015), https://www.newamerica.org/cybersecurity-initiative/national-csirts-and-their-role-in-computer-security-incident-response/.

[171] United States Telecommunications Training Institute, *at* http://www.ustti.org/about/index.php. On military professionals' newfound interest in cybersecurity, see Eneken Tikk-Ringas, Mika Kerttunen & Christopher Spirito, *Cyber Education as a Field of Military Education and Study*, 75 JOINT FORCES Q. 57 (2014).

[172] *See* MARGARET E. KECK & KATHRYN SIKKINK, ACTIVISTS BEYOND BORDERS: ADVOCACY NETWORKS IN INTERNATIONAL POLITICS (1998); Suzanne Katzenstein, *Reverse-Rhetorical Entrapment: Naming and Shaming as a Two-Way Street*, 46 VAND. J. TRANSNAT'L L. 1079 (2013); Amanda M. Murdie & David R. Davis, *Shaming and Blaming: Using Events Data to Assess the Impact of Human Rights INGOs*, 56 INT'L STUD. Q. 1 (2012); Emilie M. Hafner-Burton, *Sticks and Stones: Naming and Shaming the Human Rights Enforcement Problem*, 62 INT'L ORG. 689 (2008).

[173] *See* FRANK SCHIMMELFENNIG, THE EU, NATO AND THE INTEGRATION OF EUROPE: RULES AND RHETORIC 272 (2003).

danger of appearing hypocritical—which, again, incurs reputational and credibility costs that become mitigated by norm conformance.[174]

The Dynamic Character of Norms: The Process Is the Product

Norm cultivation culminates when the content of the norm becomes, well, normal—when the norm becomes so taken-for-granted that actors simply assume it as a social fact and part of "the way things are done." It would be a mistake, however, to assume that the formation of a fully internalized norm implies that the end product will remain fixed or unchanged. The processes by which norms form and spread guarantee them a dynamic quality.

Every time actors follow a norm, they interpret it. They have to decide what it means and what behavior it requires in the particular context at hand. Each interpretation, each episode of conformity with a norm (or failure to conform) accretes: it adds to and shapes the collective expectations of the group about what behavior is appropriate (or not). When the norm context is as varied as cybersecurity, every application of a norm is a bit different, adding rich layers of shared understanding over time about the lines of acceptable behavior in different circumstances. Rapidly changing technology only compounds this process. Because of the repeated application and interpretation of norms, not only do norms shape the behavior of actors with a given identity, but the actions of those actors shape, in turn, the contours and content of norms.[175]

Change, or the potential for change, is thus an inherent feature of all norms across all stages of development. As norms emerge and spread, the various processes—incentives, persuasion, and socialization—create repeated interactions among actors that ensure a continuous cycle of qualifications, clarifications, or alterations of the norm's meaning. Even fully internalized norms continue to evolve as context, identity, and notions of propriety change in subtle (or profound) ways. Sometimes these alterations may be unintended and unwanted by the original entrepreneurs. For example, a norm entrepreneur's version of a norm may be "captured" by a more powerful actor or by a coalition of actors who promote an altered version of the original norm, which, in turn, becomes spread and internalized within a given community.[176] But the notion that norms settle into some completely fixed and final meaning is false. Norms change with the social groups who share the norms' expectations and who apply the norms in daily life. Thus, in a critical sense norm processes *are* norm products. The processes by which norms are enacted and interpreted are integral parts of the norm's content, character, and legitimacy.

[174] *See* Martha Finnemore, *Legitimacy, Hypocrisy, and the Social Structure of Unipolarity: Why Being a Unipole Isn't All It's Cracked Up to Be*, 61 WORLD POL. 58, 72 (2009).

[175] The growing international relations literature on "practices" speaks to this process. *See*, *e.g.*, INTERNATIONAL PRACTICES (Emanuel Adler & Vincent Pouliot eds., 2011). Work on "norm enactment" provides a somewhat different understanding of these processes. *See* Antje Wiener & Uwe Puetter, *The Quality of Norms Is What Actors Make of It: Critical Constructivist Research on Norms*, 5 J. INT'L L. & INT'L REL. 1 (2009); Antje Wiener, *Enacting Meaning-in-Use: Qualitative Research on Norms and International Relations*, 35 REV. INT'L STUD. 175 (2009).

[176] In humanitarian relief circles, original apolitical "Dunantist" norms are being challenged by more "Wilsonian" norms favoring political transformation. Michael Barnett, *Humanitarianism Transformed*, 3 PERSP. ON POL. 723, 728 (2005).

Importantly, the dynamic quality of norm processes means that not all norm-promotion efforts succeed.[177] Failure remains a distinct and realistic outcome for a variety of reasons. In many contexts, "gatekeepers" have the power to decide which new norms will be advanced and which ones will not. UNICEF, for example, played this role in deciding that promoting protections for children born of war rape would not be a priority.[178] In cyberspace, actors like the United States can decide whether and when certain norm-promotion efforts should proceed. Hence, efforts to reform governance of the Internet Assigned Numbers Authority did not proceed until the United States indicated its assent to devising a new set of governance norms.[179]

Norm entrepreneurs may also fail if they face countermobilization. Norm promotion on contentious issues often energizes opposition. It can give rise to other entrepreneurs pushing different—even opposed—norms. For example, efforts at the United Nations to ban illicit trade in small arms and light weapons were stymied when countermobilization among gun rights groups managed to eviscerate their initiatives, creating what Clifford Bob calls "zombie policy."[180] In cybersecurity, as Snowden's disclosures publicized government cybersurveillance that violated the expectations of many people, privacy advocates began to push for the same privacy protections online as offline—a normative contest that remains very much in progress.[181] Contestation of this kind may eventually be resolved by defeat of one side or by changes (technological or political) that make the fight irrelevant, but resolution is by no means guaranteed. As Susan Sell has pointed out, these games of cat and mouse are driven by deep structural incentives and may be quite durable.[182]

The Pluralistic Character of Norms: Multiple Processes for Constructing Multiple Norms for Actors with Multiple Identities

Norm processes are not merely dynamic but also pluralistic in both their internal and external operations. Internally, the processes we have described are nonexclusive. Norms may form or spread by a single process (for example, socialization), but they can also emerge from multiple processes operating simultaneously. Nothing precludes a norm entrepreneur from pursuing coercion, persuasion, and socialization at the same time. Consider the U.S. push for a norm prohibiting cyberespionage for commercial advantage. U.S. officials framed the issue and sought to persuade other actors of the need for the norm because of the potential economic and national security costs. They also employed coercion via well-publicized threats to sanction

[177] *See* Jeffrey W. Legro, *Which Norms Matter?: Revisiting the "Failure" of Internationalism*, 51 INT'L ORG. 31 (1997).

[178] *See*, *e.g.*, R. Charli Carpenter, *Governing the Global Agenda: "Gatekeepers" and "Issue Adoption" in Transnational Advocacy Networks*, *in* WHO GOVERNS THE GLOBE? 202 (Deborah D. Avant, Martha Finnemore & Susan K. Sell eds., 2010); *see also* R. Charli Carpenter, *Studying Issue (Non)-adoption in Transnational Advocacy Networks*, 61 INT'L ORG. 643 (2007).

[179] *See supra* text accompanying note 100.

[180] CLIFFORD BOB, THE GLOBAL RIGHT WING AND THE CLASH OF WORLD POLITICS 109 (2012).

[181] Marianne Franklin, *Championing Human Rights on the Internet—Part Six: Summing Up, Too Much or Not Enough?*, OPENDEMOCRACY (Feb. 5, 2016), *at* https://www.opendemocracy.net/marianne-franklin/championing-human-rights-on-internet-part-six-summing-up-too-much-or-not-enough.

[182] Susan K. Sell, Cat and Mouse: Industries', States' and NGOs' Forum—Shifting in the Battle over Intellectual Property Enforcement (2009), *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1466156.

Chinese officials who engaged in the practice, and they tried socialization when they engaged in public naming and (attempted) shaming of nonconforming states, principally China.[183]

Whether actors should pursue multiple processes depends on context. In some cases, incentives, persuasion, and socialization may positively reinforce each other and advance the norm's distribution and internalization. In other cases, these tools may interact more negatively. The presence of incentives (coercion or inducements) has a documented potential to "crowd out" socialization and may even lead to higher levels of nonconformity with the norm.[184] In a famous experiment, researchers showed that imposing a fee for parents who were late to pick up their children from an Israeli day care center actually socialized those parents into thinking of the fine as a "price" for child care, rather than a "penalty" for bad behavior, leading to a rise in tardy pickups.[185]

Balancing the positive and negative consequences of the various tools to promote norms requires careful attention from cybernorm promoters, particularly when norms are likely to be contested. Scholars studying compliance with human rights norms argue that different processes will be at work in different stages of the norm-adoption and internalization processes.[186] Actors may start out resistant to a new norm and may deny the norm's applicability altogether. Coercion plays a large role at these contentious stages, and states have obvious advantages in the use of such tools. In the case of human rights and democracy norms, states have often used violent repression against norm promoters. Civil society groups, often promoting very different norms, may take to the streets or file lawsuits. Over time, tactical concessions may be made by states resisting the norm; that is, they may minimally conform for instrumental reasons, paying lip service to the norm to satisfy promoters, without actually changing beliefs or engaging in any more norm-conforming behavior than necessary. This tactical or insincere conformity may continue for some time, but if compliance continues, interactions may move toward dialogue, with persuasion and different forms of socialization taking center stage. Thus, moving actors along the continuum of norm acceptance requires attention to the full tool kit.

The array of norm processes at work multiplies when we look more externally at the larger systems or sets of norms that may coexist. Actors with a given identity regularly associate themselves with multiple norms. Some of those norms may coexist harmoniously, but others may conflict or compete, requiring intersubjective adjustments within the community on issues of priority or context (that is, whether a certain norm must give way when it conflicts with another

[183] Ellen Nakashima & Steven Mufson, *U.S., China Vow Not to Engage in Economic Cyberespionage*, WASH. POST (Sept. 25, 2015); Matt Sheehan, *China Mocks U.S. "Hypocrisy" on Hacking Charges*, WORLD POST (May 20, 2014), *at* http://www.huffingtonpost.com/2014/05/20/china-cyber-spying_n_5356072.html.

[184] GOODMAN & JINKS, *supra* note 155, at 172.

[185] *See* Uri Gneezy & Aldo Rustichini, *A Fine Is a Price*, 29 J. LEGAL STUD. 1 (2000).

[186] Thomas Risse & Stephen C. Ropp, *Introduction and Overview*, *in* THE PERSISTENT POWER OF HUMAN RIGHTS: FROM COMMITMENT TO COMPLIANCE 3 (Thomas Risse, Stephen C. Ropp & Kathryn Sikkink eds., 2013); Risse & Sikkink, *supra* note 122, at 17–35. Risse, Ropp, and Sikkink's "spiral model" was developed to describe promotion of human rights norms that are often highly contentious, especially when governments view human rights as a threat to regime stability. Some cybernorms may be analogous, like Chinese and Russian definitions of "cybersecurity" as "information security," which allow (or require) state control of communications' content. Other cybernorms may be less contentious and more in the nature of a coordination problem; for example, TCP/IP norms derive from a desire for interconnectivity. A more mixed-motive example might be using the Secure Socket Layer to ensure encrypted communications between a server and a client. Promotion and adherence in each of these cases may follow a different trajectory and go through different stages.

norm, or whether certain norms govern in particular contexts).[187] In using ICTs, for example, states continue to grapple with how to integrate the propriety of cyber surveillance with normative expectations that states should respect both private property rights (for example, intellectual property) and individual civil liberties.

To complicate matters further, all actors, including states, have multiple identities—they associate with different communities simultaneously. A state like the United States, for example, may identify itself simultaneously as part of the community of *all* states, the community of *liberal-democratic* states, and the community of the *most powerful* states. Such different groups, of course, will each have different norms, ones that may be partially or completely incompatible. This reality complicates normative processes and creates uncertainty about which identity (and thus which norms) an actor will prioritize in any given situation. But it also reinforces our basic thesis: understanding cybernorms cannot depend entirely on an articulation of their contents. Paying attention to the mechanisms and pathways by which norms form and operate must be an integral part of any conversation about the substance of what they say.

III. THE NOVELTY OF CYBERSPACE FOR NORMATIVE PROCESSES

We now know a great deal about how to cultivate robust, pro-social norms in diverse regulatory spaces. We know that *norm entrepreneurs* can be crucial, especially in the early stages of norm emergence. We know that the *organizational platform* from which norms are pushed can strongly shape both the content of the norm and its appeal (or not) to target audiences. We know that *grafting* new norms onto existing norms or processes can enhance legitimacy by making them seem like logical outgrowths of accepted beliefs or institutions. And we know that *incentives*, *persuasion*, and *socialization* all play roles in the acceptance and spread of new norms.

But is any of this knowledge applicable to cyber? Is cyberspace unique in ways that doom norm construction? Analysts often stress the unique features of ICTs that create distinctive challenges for regulation, in general, and for norm cultivation, in particular. Digital communication is said to be too complex for easy governance. Its technologies change too quickly. The actors involved are too diverse and want incompatible things.

We believe these fears are overstated. Cultivating robust pro-social norms is difficult in any complex regulatory arena. Managing climate change, promoting democracy, and implementing transitional justice all require new norms that involve diverse actors who want different—usually incompatible—things. All involve rapidly changing contexts and situations, and all involve a great deal of uncertainty about both the present and the future. Certainly, cyberspace has distinctive features. That should not blind us, however, from recognizing its commonalities with other issues from which we might learn. In this section we assess some common claims about cyberspace's putative novelty; our goal is to understand better what really is new and what features cybersecurity shares with other norm-cultivation projects.

[187] The "regime complex" literature also addresses issues raised by multiple, often competing configurations of norms. *See* Karen J. Alter & Sophie Meunier, *The Politics of International Regime Complexity*, 7 PERSP. ON POL. 13 (2009); Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources*, 58 INT'L ORG. 277 (2004); Laurence R. Helfer, *Regime Shifting: The TRIPs Agreement and New Dynamics of International Intellectual Property Lawmaking*, 29 YALE J. INT'L L. 1 (2004).

Does Its Technical Architecture Make Cyberspace Unique?

Several features of cyberspace's technical architecture are often cited as obstacles to successful governance or effective regulation. Specifically, the *speed*, *scale,* and *secrecy* created by ICTs are often identified as unique challenges for governance.[188]

Speed of change. Is technology changing so quickly in cyberspace that norms cannot keep up? Rapid technological change has been a hallmark of digital communication since its inception. In just two decades we have moved from a world of dial-up connections linking mostly university computers to billions of individuals using broadband and cloud-based storage on handheld devices. Moore's law suggests that processor speeds double roughly every two years, a pattern that has held true for more than four decades.[189] And soon we are told to expect the "Internet of Things," a world where everything—our houses, our forests, our medical devices—will have an online presence.[190]

If technology changes this quickly, how could norms possibly keep up? Norms often take time to evolve, in no small part because norms move only at the pace of human cognition and interaction. After all, norms are shared human understandings. People—in particular, large groups of people—can hardly be expected to update their understandings, much less work through the social processes of sharing and institutionalizing them, at the same speed as microprocessors.[191]

The pace of technological change in cyberspace may be unique, but things also move quickly in other regulatory contexts. The spread of epidemic disease, for example, has some of the same exponential growth properties as Moore's law. Biological viruses also mutate, further frustrating our efforts to control their spread, just as technological changes can frustrate governance. During the recent Ebola outbreak, that virus spread exponentially, and influenza is notorious for its rapid rates of mutation, making effective flu shots and regulatory strategies challenging.[192] These characteristics make it difficult to control epidemics, but public health officials have not given up on norms as part of the solution; indeed, quite the reverse. They use the

[188] *See*, *e.g.*, Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1283 (2013) (noting that rate of technological advancement contributes to cyberspace being a "unique space").

[189] Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, 86 PROC. IEEE 82 (1998), *reprinted from* ELECTRONICS, Apr. 19, 1965, at 114. *But see* Don Clark, *Moore's Law Shows Its Age*, WALL ST. J. (Apr. 17, 2015), *at* http://www.wsj.com/articles/moores-law-runs-out-of-gas-1429282819 (suggesting that doubling rate is slowing).

[190] *See supra* note 6; J. M. Porup, *Malware in the Hospital*, SLATE (Jan. 25, 2016), *at* http://www.slate.com/articles/technology/future_tense/2016/01/malware_not_malicious_hackers_is_the_biggest_danger_to_internet_connected.html; Adrienne LaFrance, *When You Give a Tree an Email Address*, ATLANTIC (July 10, 2015), *at* http://www.theatlantic.com/technology/archive/2015/07/when-you-give-a-tree-an-email-address/398210/.

[191] As a result, some norms have taken years, if not decades, to form and spread (for example, abolition). *See*, *e.g.,* ROBIN BLACKBURN, THE OVERTHROW OF COLONIAL SLAVERY, 1776–1848 (1988).

[192] Geraldo Chowell, Cécile Viboud, James M. Hyman & Lone Simonsen, *The Western Africa Ebola Virus Disease Epidemic Exhibits Both Global Exponential and Local Polynomial Growth Rates*, PLOS CURRENTS: OUTBREAKS (Jan. 21, 2015), *at* http://currents.plos.org/outbreaks/article/the-western-africa-ebola-virus-disease-epidemic-exhibits-both-global-exponential-and-local-polynomial-growth-rates/; Patrick Honner, *Exponential Outbreaks: The Mathematics of Epidemics*, N.Y. TIMES (Nov. 5, 2014), *at* http://learning.blogs.nytimes.com/2014/11/05/exponential-outbreaks-the-mathematics-of-epidemics/.

urgency of pandemic disease to push acceptance of behavioral changes that might stem a disease's spread.[193]

Scale. Does the pervasiveness of ICTs—the fact that they are so widely distributed geographically and have so many users of varied types—present unique challenges?[194] Digital communications now reach virtually every corner of the globe, and ICT use has become ubiquitous, from household appliances to power plants. This distribution means that everyone is, in some way, an "actor" in governing cyberspace. The sheer scope and scale of the technology's reach would seem to create an impossible array of stakeholders and participants in norm-development processes.

Again, there is an element of truth here, but such pervasiveness is not without precedent, and some obvious coping strategies are available. Carbon emissions are at least as pervasive as ICTs, but this pervasiveness has not halted efforts to develop norms relating to emissions.[195] Admittedly, that road has been difficult—just as the road to cybernorms will be—but we certainly have witnessed pluralistic, multistakeholder processes that generated behavioral changes, including changed expectations and attitudes, even if that change is not as rapid as we want or need.

Secrecy. Does the anonymity of some cyber behavior make fostering shared expectations more difficult? After all, if people do not know who is doing what on the Internet, conventional methods of socialization, persuasion, and incentives might be difficult to implement.[196]

Problems with "attribution"—that is, knowing which actor is responsible for specific Internet activities—are often cited as a distinctive feature of cyberspace.[197] Anonymity itself is neither good nor bad, however, and we may even like some forms of the "attribution problem." For example, Tor technology allows dissidents and human rights activists to circumvent censorship and maintain the privacy of their communications.[198] Other forms of the attribution problem are more worrisome. Criminals obviously have found many ways to turn attribution problems to their advantage, evading responsibility for malicious activity. So, too, have governments, who may find it useful to hide their identities online and often, too, what they are doing.[199] In the military realm, effective deterrence policies are hard to implement in the absence of attribution since, without knowing who did what, states (or other actors) cannot punish security violators. Scholars are consequently having lively debates about the extent to

[193] *See* Amy Maxmen, *How the Fight Against Ebola Tested a Culture's Traditions*, NAT'L GEOGRAPHIC (Jan. 30, 2015), *at* http://news.nationalgeographic.com/2015/01/150130-ebola-virus-outbreak-epidemic-sierra-leone-funerals/.

[194] Nevertheless, half the world—57 percent, or 4.2 billion people—still lacks regular Internet access. BROADBAND COMMISSION FOR DIGITAL DEVELOPMENT, THE STATE OF BROADBAND 2015: BROADBAND AS A FOUNDATION FOR SUSTAINABLE DEVELOPMENT 8 (2015), *at* http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf.

[195] *See* Adoption of the Paris Agreement, UN Doc. FCCC/CP/2015/L.9/Rev.1 (Dec. 12, 2015).

[196] As the adage goes, "On the Internet, nobody knows you're a dog." *See* https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog#/media/File:Internet_dog.jpg. The original cartoon, by Peter Steiner, was published July 5, 1993, in the *New Yorker*.

[197] *See supra* notes 69–72 and accompanying text.

[198] Tor Project, *Users of Tor*, *at* https://www.torproject.org/about/torusers.html.en.

[199] Kristen Eichensehr, *Cyber Attribution Problems—Not Just Who, But What*, JUST SECURITY (Dec. 11, 2014), *at* https://www.justsecurity.org/18334/cyber-attribution-problems-not-who/.

which (and the manner in which) cyberspace's architecture might require rethinking deterrence policies.[200]

Secrecy and attribution problems may complicate norm creation, but their novelty and effects should not be overstated. Attribution problems have long plagued other global problems like terrorism and proxy actors, even before the advent of the Internet. So-called false-flag attacks by governments also have a long history.[201] Contemporary ICTs may make these attacks easier on some dimensions (and more common), but the basic logic of the secrecy challenge to governance, rule making, and norms is not unique to cyberspace.[202]

The bigger challenge posed by secrecy and anonymity is probably to enforcement, not to norm creation. Sneak attacks and malicious activity are widely viewed as bad, and shared expectations that such acts should be condemned are quite robust. Technological means to speed up attribution and refine its precision are also moving forward rapidly and may lessen this problem. While most attribution is done with a combination of technological forensics and other forms of intelligence—a process that often takes longer than policy makers might like—concerns about the severity of this problem seem to be lessening.[203]

Do the Internet's Governance Mechanisms Make It Unique?

Since its creation, the Internet has developed an array of governing modalities that enable it to function as it does. Do these existing arrangements pose unique challenges for the cultivation of cybernorms?

Cyberspace versus sovereignty. The Internet is not organized around national borders or Westphalian sovereignty norms. The "packet-switched" network divides data into lots of smaller pieces, attaches addressing information to them, and routes them separately along any number of paths to their destination, where the data is reassembled into its original form. These routes have little connection to the contours of physical or political landscapes. Indeed, the term *cyberspace* exists in part to convey this detachment from territorial borders and to emphasize the way that communications have become decoupled from physical space.[204]

Do cyberspace's nonterritorial features somehow limit states' ability to control what goes on there? Many users and observers have been taken with this idea. Since the earliest days, a significant user population has embraced the Internet as a realm of freedom from the kinds of regulation and control that sovereign states impose in physical space.[205] If states were actually unable to exercise their defining monopoly on legitimate use of coercion in cyberspace, that inability might indeed be a distinctive and novel feature.

[200] Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4 (2015); Jon R. Lindsay, *Stuxnet and the Limits of Cyber Warfare*, 22 SECURITY STUD. 365 (2013).

[201] *53 Admitted False Flag Attacks*, WASHINGTONSBLOG (Feb. 23, 2015), *at* http://www.washingtonsblog.com/2015/02/x-admitted-false-flag-attacks.html.

[202] If anything, "Big Data" and the "Internet of Things" make it harder to remain anonymous, given how they track and gather data. *See supra* notes 6, 190; Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014).

[203] *See* Bruce Schneier, *Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle*, CHRISTIAN SCI. MONITOR (Mar. 4, 2015), *at* http://www.csmonitor.com/About/People/Bruce-Schneier.

[204] Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 210–11 (2007).

[205] *See, e.g.*, John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), *at* https://www.eff.org/cyberspace-independence; David R. Johnson & David Post, *Law and Borders—the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375–76 (1996).

For the most part, though, this notion is a myth. States can and do control cyberspace when it suits them—and often with a heavy hand.[206] One obvious point of leverage is that crucial pieces of the ICT infrastructure are physical and have to be anchored on terra firma. Servers and undersea cables, for example, have a tangible physical existence; cables are anchored, and servers are located in some state somewhere. States use these physical features of cyberspace, among other tools, to exert power. Proposals for data-localization legislation, which requires communication to be routed through servers located in particular states, has proliferated around the world—specifically, in Brazil, Russia, and the European Union.[207] But these physical links are not the only routes to Internet control. The Great Chinese Firewall has been successful at configuring networks and filters to control content viewed by China's citizens.[208] And, of course, the notion that some domains—the oceans, outer space, Antarctica—lie outside state boundaries is not new in international law. States have nonetheless crafted rules, and norms have formed, to govern those regions.[209]

States do not own the Internet. When confronted with other types of security threats, states build—and therefore own and control—tools to combat that threat. States build armies and aircraft carriers to defeat enemies and win wars. They build nuclear arsenals to deter attacks. In that more conventional world of kinetic warfare, the tools belong to states that can deploy them as their governments see fit. But in cyberspace, governments often do not own the networks and ICT resources; private companies do. This pattern is especially common in the capitalist OECD countries, where connectivity is most dense.[210] Although the U.S. military has its own networks, which it maintains, much of the military's work and virtually all of the U.S. government's work is done over commercial networks owned and maintained by nonstate, private corporations.

If states do not own the ICT resources, does that situation pose an obstacle to regulation or norm creation in cyberspace? It is hard to see why it would. States regulate privately owned resources all the time, including resource flows that cross national boundaries. Law, norms, and rules are dense around maritime issues, transboundary trade, extractive industries, and human trafficking, to name just a few.[211]

"Code is law" or "Code is norm"? The notion that the technical community has created a "law" unto itself in cyberspace was widely popular in the Internet's early days. Code written by technologists created new "spaces" and sites of human activity. Code shapes possibilities for human action, enabling some types of action and prohibiting others. If technologists can create their

[206] *See*, *e.g.*, Chris C. Demchak & Peter Dombrowksi, *Rise of a Cybered Westphalian Age*, 5 STRATEGIC STUD. Q. 32 (2011); JACK L. GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?, at xii (2006); Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 359–61 (2003).

[207] *See* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677 (2015).

[208] Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J. L. SCI. & TECH. 125 (2012).

[209] *See* Duncan B. Hollis, Stewardship Versus Sovereignty? International Law and the Apportionment of Cyberspace 6–7 (paper prepared for the Cyber Dialogue forum, Toronto, Canada, March 18–19, 2012) (on file with authors).

[210] *See generally* Alexander Klimburg, *Mobilising Cyber Power*, 53 SURVIVAL 41 (2011) (noting, in contrast, how Chinese and Russian governments regularly assume that they can control nonstate actors).

[211] *See*, *e.g.*, UN Convention on the Law of the Sea, Dec. 10, 1982, 1833 UNTS 3; Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 UNTS 154; Extractive Industries Transparency Initiative, *at* https://eiti.org; *see also* Virginia Haufler, *Disclosure as Governance: The Extractive Industries Transparency Initiative and Resource Management in the Developing World*, 10 GLOBAL ENVTL. POL. 53 (2012).

own world with its own rules through the code they write ("regulation by code"), what role is left for noncode governance mechanisms like government regulations or social norms? Lessig first aired these issues more than a decade ago, and others have expanded on the theme since.[212]

Again, although these claims reflect important insights, they are also easily overstated. Code is written by technologists who themselves work in communities governed by a dense fabric of professional or cultural norms that tell them what constitutes "good code" or "elegant solutions" to problems. These norms also dispose technologists toward particular views of the role that digital technology can or should play in society more generally. If code is a governing mechanism unto itself, it is one that rests on social norms deeply held by its authors.[213] There is also no a priori reason why code must be written to evade state regulation. Code could just as easily be written to facilitate state control—and often is, as current debates over back doors in software illustrate.[214] At the same time, the technologist community often has a strong voice in debates about whether and how states should exercise their power to regulate and legislate.[215] Cyber issues are hardly the only ones on which technological communities wield major influence. Technical experts are key players in other global problems, as in debates on nuclear, ecological, and financial regulation.[216]

The multistakeholder model of cyber governance. Cyberspace has developed its own governance modalities, at the center of which is a "multistakeholder model" most often applied to the Internet: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[217] This pluralistic set of processes, which has its roots in the Internet's early role as a collaborative research tool for technologists, contrasts sharply with most state regulatory frameworks. In the multistakeholder model, states are only one "authority" among many. Allegiance to this multistakeholder model is strong, particularly among technologists, and suspicion of top-down regulation by states runs deep. Could these attitudes pose a unique or insurmountable obstacle to norm cultivation or regulation more generally?

Hardly. First, multistakeholderism is not the governance mechanism for all aspects of cyberspace, especially cybersecurity. As Laura DeNardis describes it, Internet governance is an enormously complex array of diverse tasks carried out by different actors.[218] The multistakeholder model is central to some of these; for example, it is central to carrying out the Internet Assigned

[212] LESSIG, *supra* note 118; *see also* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008); LAWRENCE LESSIG, CODE: VERSION 2.0 (2006); Tim Wu, *When Code Isn't Law*, 89 VA L. REV. 679 (2003).

[213] *See generally* STEVEN WEBER, THE SUCCESS OF OPEN SOURCE (2004).

[214] *See supra* notes 1–5, 15, 116, 142–44, and accompanying text; *When Back Doors Backfire*, ECONOMIST (Jan. 2, 2016), *at* http://www.economist.com/news/leaders/21684783-some-spy-agencies-favour-back-doors-encryption-software-who-will-use-them-when-back. Lessig also makes this point. LESSIG, *supra* note 118, ch. 5.

[215] *See*, *e.g.*, Sarah McBride & Lisa Richwine, *Epic Clash: Silicon Valley Blindsides Hollywood on Piracy*, REUTERS (Jan. 22, 2012), *at* http://www.reuters.com/article/us-congress-piracy-idUSTRE80L0VS20120122.

[216] *See generally*, Peter M. Haas, *Introduction: Epistemic Communities and International Policy Coordination*, 46 INT'L ORG. 1 (1992).

[217] Tunis Agenda for the Information Society 6, UN Doc. WSIS-05/TUNIS/DOC6 (Rev.1)-E (Nov. 18, 2005), *at* http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.pdf. For more on the multistakeholder definition, see TIM MAURER, CYBER NORM EMERGENCE AT THE UNITED NATIONS (2011), *at* http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

[218] *See* LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE, ch. 1 (2014).

Numbers Authority functions and the functioning of the Internet Corporation for Assigned Names and Numbers. It is much less relevant to the Wassenaar Arrangement and its recently expanded export controls for a variety of surveillance technologies.[219] Other features of Internet governance have different mixes of multistakeholder governance with more traditional state-led regulation.

Multistakeholder models are also not unique to cyberspace. Governance models involving diverse participation by diverse actors first emerged in environmental politics and have since been adopted in a wide variety of contexts, including public health—where there is the Joint UN Programme on HIV/AIDS and GAVI, the Vaccine Alliance—and securities regulation, with the International Organization of Securities Commissions.[220] Norm cultivation has been a major focus of all of these multistakeholder arrangements. Participants can (and do) claim that inclusiveness actually makes it easier to spread new norms since participation in norm development creates a sense of ownership that then facilitates compliance and institutionalization.

IV. Strategic Social Construction: The Trade-Offs in Cybernorm Promotion

The previous sections demonstrate that norm processes are both significant and relevant to cybersecurity. But what can states and other stakeholders do with these findings? Our thesis remains simple and straightforward: if robust norm processes—the means by which norms are constructed, promoted, and institutionalized—are integral parts of successful cybernorms, then cybernorm proponents must devote as much attention to these processes as they have to negotiating desired behavioral goals. Creating good processes is not easy, however. It requires effort, foresight, and recognition of the trade-offs likely to confront norm proponents.

We envision the cultivation of new cybernorms as an exercise in *strategic social construction*. Current calls for cybernorms suggest little confidence in existing norms' adequacy to manage this evolving technology. Actors will have to construct new cybernorms through individual or collective acts of entrepreneurship. Ensuring new norms are reliable (not to mention effective) will require complex strategic choices involving (1) the contexts, (2) norm elements, and (3) tools of influence introduced above.[221] Actors pushing for cybernorms are already making some of these choices, but the extent to which they are doing so in a conscious, let alone strategic, manner is unclear.

In this section, we highlight some of the most obvious consequences and trade-offs in play for advancing cybernorms. We make no pretense that we can identify which choices— or combination of choices—will lead to successful cybernorms. Our more modest goal is to push actors to make more careful and considered choices. We also set the stage for further research assessing the effectiveness of different strategies for the promotion of norms, in general, and cybernorms, in particular.

[219] Jennifer Granick, *Changes to Export Control Arrangement Apply to Computer Exploits and More* (Jan. 15, 2014), *at* http://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more.

[220] Mark Raymond & Laura DeNardis, *Multistakeholderism: Anatomy of an Inchoate Global Institution*, 7 Int'l Theory 572 (2015).

[221] *See supra* parts I (contexts) and II (normative elements and tools).

Choosing and Framing the Context for Cybernorms

Strategic social construction of cybernorms begins with framing. As we demonstrated in part I, cybersecurity is not a monolithic issue. It arises in multiple contexts involving varied actors and technologies. Thus, norm promoters must first decide *which* problems require attention. Should priority go to securing ICTs from the causes of insecurity? If so, which of the three conditions that we identified—namely, vulnerabilities, access issues, and malware payloads—should become the focus of attention? Or is the problem better framed in terms of the harmful effects that victims suffer—and, if so, which harms pertaining to confidentiality, integrity, access, or more indirect effects, and for which victims? Or perhaps the most important problem should be understood in terms of bad actors, whether hackers, hacktivists, cybercriminals, militaries, or intelligence agencies?

Selecting a problem for normative attention necessarily involves selecting a context since different contexts set different parameters for normative solutions. Consider, for example, the dangers of military operations against critical civilian infrastructure. Framing the problem as actors (for example, militaries) behaving badly suggests that any new norm should redraw the lines of appropriate military behavior. But if the problem is recast in terms of its technical causes or indirect effects, then the norm would focus on defensive behavior by critical-infrastructure industries themselves, such as doing more to limit access to their networks or improving their resilience to the effects of operations affecting their systems' integrity or availability. Thus, how cybernorm entrepreneurs choose to frame their problems can set processes of norm development along very different pathways.

Importantly, the selected context will shape the roster of potential players whom the norm might identify as responsible for solving a problem. Consider the problem of zero-day vulnerabilities. Software developers could engage in greater due diligence before releasing their products; security researchers could have heightened responsibilities to disclose vulnerabilities; ISPs could identify and notify infected users of vulnerabilities once known; or law enforcement officials could target those trading in vulnerabilities on the black market. Thus, careful framing is required within any given context to identify which group is best suited to deal with the problem and which groups will be left outside the norm-promotion process.

A significant aspect of framing is *linking* cybersecurity problems to larger issues that easily garner attention and resources. The problem of cybercriminals is regularly cast in terms of economic costs, creating additional support for cybernorm construction that shores up the financial security of firms and, with them, national and global economies. Encryption is regularly linked to privacy, giving pro-encryption norms the overall benefits that a pro-privacy position may provide. Of course, many contexts allow multiple linkages; the problem of cyberespionage, for example, has an economic tie-in in terms of its financial losses, a privacy linkage in terms of data breaches, and a national security agenda in cases targeting the U.S. government or its personnel. President Obama invoked multiple links when he chose to describe cyber insecurity as "one of the most serious economic and national security challenges we face as a nation";[222] doing so tied the issue to two of the larger narratives with which he—and the nation—are most concerned.

[222] Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *at* https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

Strategic selection of contexts may involve complicated trade-offs for norm entrepreneurs. For example, should they try to cultivate norms in a limited context—one region, one industry—where actors seem favorably disposed and chances of success might be higher, but where the "reach" of the norms will be less (for example, cultivating military cybernorms within the North Atlantic Treaty Organization only)? Or is it better to tackle the cyberthreat globally, perhaps through the United Nations, where there will be more disagreement and the norm may be less demanding, but where the reach might be broader?

Further complications arise when norm entrepreneurs pursue multiple frames simultaneously—for example, targeting the behavior of both militaries and cybersecurity industries to reduce the overall risk of harm.[223] Framing the same problem in multiple ways could increase the chances that more actors adjust their behavior to deal with the problem. But this approach could also create a free-rider problem if the cybersecurity industry decides that the real problem is with the military and waits for the military to act, while the military reaches the opposite conclusion.

Similar trade-offs exist in linking a single problem or cybernorm to multiple narratives. Sometimes, doing so reinforces the issue's significance, as President Obama's statements did. But making multiple linkages may also create new risks when narratives diverge or conflict. Consider the problem of confidentiality losses and the propriety of encrypting data to avoid them. For a time, the pro-encryption position tied in logically with economic security (protecting commercial intellectual property and reducing liability for data breaches), privacy (protecting private communications among users), and national security (protecting the nation's secrets). But after the 2015 terrorist attacks in Paris and San Bernardino, the national security narrative shifted, with suggestions that encrypted communications were themselves a national security threat.[224] This "encryption-as-threat" narrative is in some tension with the earlier narratives and consequently raises issues of priority. For those favoring national security, this linkage may therefore end up reverberating back to destabilize the pro-encryption norm itself.

So far, we have discussed strategic social construction in the context of a single problem—namely, where norm entrepreneurs make choices and accept trade-offs to form, spread, or internalize a discrete norm. But the complexity of cybersecurity adds significantly to the complexity of our portrait. With so many insecurities in cyberspace, any framing and linking in this area requires attention to multiple problems and thus multiple cybernorms. Norm entrepreneurs must begin to think about their strategic choices holistically; they must consider not just individual norms in isolation but the larger fabric of norms. Certain choices may be synergistic, with the framing and linking of one problem facilitating the construction of a whole set of related cybernorms. For example, the decision to emphasize a norm that states should apply international law to their operations in cyberspace opens the door to a whole array of related cybernorms, as illustrated by the *Tallinn Manual*'s detailed coverage.[225] But other choices may

[223] The United States, for example, has pushed states at the GGE to agree not to target critical infrastructure, while seeking heightened critical industry cybersecurity at home. *See*, *e.g.*, Grigsby, *supra* note 148; *Cybersecurity Framework*, *supra* note 93.

[224] *See supra* notes 142–44 and accompanying text.

[225] In its 2013 report, the GGE agreed that "International law, and in particular the Charter of the United Nations, is applicable" to the "ICT environment." Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A68/156/Add.1 (Sept. 9, 2013). Attempts to elaborate on that statement in the 2015 report failed. *See* David Fidler, *The GGE on Cybersecurity: How International Law Applies to Cyberspace*, NET POLITICS (Apr. 14, 2015), *at* http://blogs.cfr.org/cyber/2015/04/14/the-un-gge-on-

interact more negatively. Chosen norms may end up competing for attention among the concerned communities or, in the worst case, may conflict and undermine each other, thereby creating a less secure environment. If, for example, military offensive cyber-operations like Stuxnet are appropriate, that choice affects, if not undermines, the appropriateness of all sorts of norms regarding the integrity and availability of ICTs generally.

Picking Norm Ingredients: Trade-Offs in Identity, Behavior, Propriety, and Expectations

Strategic social construction of norms does not end with framing and linking. Norm entrepreneurs must also make significant choices about the structure and character of the cybernorms that they plan to pursue. They must do so, of course, in light of extant circumstances, building from the existing normative heterogeneity that we explored in part II. The four ingredients we introduced there—identity, behavior, propriety, and expectations—provide key inflexion points for additional decisions that affect the construction of cybernorms.[226] The precise future impacts may be difficult to discern in any particular case. Nonetheless, many of these decisions involve clear trade-offs—identifiable risks of, and potential rewards from, pursuing a particular course. Awareness of these risks and rewards presents sophisticated actors with strategic choices about how best to achieve the successful adoption, spread, and internalization of desired cybernorms.

Identity: Whom does the cybernorm govern? Recall that norms take the form "actor of identity X should do Y." Entrepreneurs must decide which group should change its behavior when promulgating a new norm. As we noted above, framing and linking narrow the range of groups whose identity matters for addressing a particular cybersecurity problem, but the specification of broad categories, such as states, may be insufficiently focused to achieve desired goals. For states, there are at least three options to consider—bilateral pairings, plurilateral "silos," and global (with a diverse range of states or groups)—each of which may produce a range of advantages and disadvantages.

First, two states could serve as the group that shares a particular cybernorm. In other words, cybernorm identities can be constructed bilaterally, one relationship at a time. The United States ultimately opted for this approach when China joined it in pronouncing a norm against cyberespionage for commercial advantage.[227] Going bilateral has clear advantages. Adoption of the norm may prove easier when only one other party needs to share the behavioral expectation. Transaction costs are relatively low, as are the costs of obtaining information about each side's interests and values. And in most cases a bilateral beginning does not foreclose options to expand the norm later: if the pair subsequently chooses to become entrepreneurial, they can create conditions for broader acceptance of their norm. Successful bilateral cybernorms can produce mimicry, particularly if the states involved are high status, as the espionage case illustrates. Once the United States and China adopted a norm against commercial cyberespionage,

cyber-issues-how-international-law-applies-to-cyberspace/. The *Tallinn Manual*, by contrast, had more success in elaborating an array of norms based on this first one. TALLINN MANUAL, *supra* note 11, at 3, 13.

[226] *See supra* notes 85–125 and accompanying text.

[227] *See supra* note 12 and accompanying text.

both Germany and the United Kingdom quickly undertook their own bilateral negotiations with China—moves that later led the entire G-20 to adopt the norm.[228]

The cascade witnessed in the U.S-China espionage case aside, other bilateral norms may remain limited in their reach. Indeed, third states may resist accepting a bilateral norm either because they resent their initial exclusion or because they believe the bilateral norm reflects specialized interests or values that do not extend more broadly. China and Russia's newly shared expectations of cooperation against technology that destabilizes the society or interferes with internal affairs derives, at least in part, from both governments' concerns about regime stability, conditions that do not motivate most Western states.[229] Even when bilateral norms do cascade, they may cascade in further bilateral pairings, leading potentially to different norms than those that a group might adopt if acting collectively. For example, developing states have agreed to thousands of bilateral investment treaties establishing a norm that compensation for expropriation must be "prompt, adequate, and effective" even as developing states, acting collectively at the United Nations, opposed and sought to dethrone that norm as one of customary international law.[230]

In lieu of a bilateral pairing, norm entrepreneurs might choose to situate cybernorms in a plurilateral silo—that is, a group of regional or like-minded states, such as the European Union, Shanghai Cooperation Organization, or Freedom Online Coalition.[231] Norm siloing has obvious upsides. It can create islands of normativity that serve the groups' interests or values. If the shared interests that underpin the silo group are extensive, the islands' norms can become dense and deep.[232] And like bilateral pairings, reliable and effective norms may exert a pull on other states outside the silo, allowing cybernorms to cascade into a broader subject group. Witness, for example, how the Cybercrime Convention's membership has broadened considerably beyond the Council of Europe, which negotiated it.[233]

But pursuing norm silos also presents certain risks. Groups that are not like-minded may generate different sets of cybernorms, leading to competing or conflicting islands of normativity, with no ready-made tools to bridge the two (or more) camps. Compare, for example, the Freedom Online Coalition's support for norms of free expression online to the Shanghai Cooperation Organization's norms for limiting subversive political speech.[234] Depending on

[228] *See supra* notes 12, 89, 113, 151, and accompanying text; Stefan Nicola, *China Working to Halt Commercial Cyberwar in Deal with Germany*, BLOOMBERG NEWS (Oct. 29, 2015), *at* http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany.

[229] *See* Cory Bennett, *Russia, China United with Major Cyber Pact*, HILL (May 8, 2015), *at* http://thehill.com/policy/cybersecurity/241453-russia-china-unit-with-major-cyber-pact; Russia-China Agreement, *supra* note 12.

[230] Andrew T. Guzman, *Why LDCs Sign Treaties That Hurt Them: Explaining the Popularity of Bilateral Investment Treaties*, 38 VA. J. INT'L L. 639, 643 (1998).

[231] *See* Freedom Online Coalition, *at* https://www.freedomonlinecoalition.com.

[232] Depth refers to the extent to which actors depart from what they would have done in the norm's absence. *See* GOODMAN & JINKS, *supra* note 155, at 97; ANDREW T. GUZMAN, HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY 154–56 (2008).

[233] As of August 1, 2016, the Budapest Convention, *supra* note 11, had forty-nine parties, including, most recently, Australia, Canada, and Japan. *See Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime*, *at* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG. The African Union treaty may also be a concrete example of mimicking, hoping to replicate the Budapest Convention's success. African Union Convention on Cyber Security and Personal Data Protection, *supra* note 87.

[234] *See* Freedom Online Coalition, *WG-1—an Internet Free and Secure*, *at* https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/ (recommending "greater stakeholder-driven and human

the cybersecurity problem, such competition among norm silos may prove destabilizing, particularly on the Internet, where ICT technology is presumably shared globally, among all users.[235]

Instead of choosing to pair or silo, states could also go global, opting for more universal processes. These processes could involve states or even some larger multistakeholder group like NETmundial that includes states alongside other stakeholders.[236] Processes to construct universal norms need not include all states as participants, particularly if conducted on a legitimate universalistic platform. Thus, the GGE comprised (in its most recent incarnation) twenty states, operating under UN auspices, that proffered norms for universal purposes.[237]

The upside of going global is that, if successful, the norm constructed can stabilize the whole "system" rather than simply islands of it. Universal norms may reduce both conflicts among competing norms and the inefficiencies (or insecurities) that come with fragmented sets of rules. For cybersecurity issues requiring global cooperation (for example, the security of critical Internet infrastructure, such as the Internet Assigned Numbers Authority), global norms may be the only option. The downside is that achieving global arrangements can require a lot of time, effort, and money; for example, the GGE has been at work off and on since 1998.[238] Broad participation may also yield shallow, "lowest common denominator" norms if differences in interests and values are so great as to preclude more robust intersubjective understandings. Looking at the GGE again, states have had great difficulty moving beyond the norm that international law, including the UN Charter, applies in cyberspace. At present, more specific norms on how international law applies are still absent from UN processes.[239]

Behavior: What does the norm say and where does it say it? When states and other stakeholders give attention to the strategic social construction of cybernorms, they have thus far focused on what the norms say—the substantive content of what they tell actors to do (or not do). But they also must choose from a range of regulatory forms (including prohibitions, requirements, or permissions) and types (rules, standards, or principles).[240]

The chosen structure of the norm may influence chances for uptake and internalization. The precision of rules, for example, imposes a rigidity that can make them unworkable as technology or circumstances change.[241] Conversely, actors may have trouble applying standards to themselves absent third-party enforcement, a common situation in cyberspace. Norms creating obligations that exceed the capabilities (or perceived capabilities) of actors will obviously encounter resistance, nonconformance, or both, and thus would require additional elements—exceptions, assistance, delayed compliance schedules—to win support.

rights respecting approaches to cybersecurity"); Revised SCO Code of Conduct, *supra* note 11, para. 2(3) (emphasizing norms against using ICT to "interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability").

[235] Compare Wassenaar's attempts to reduce trade in surveillance technology with norms of states like China that have such systems baked into their technological architecture. *See* Wassenaar Arrangement, *supra* note 13; Lee & Liu, *supra* note 208, at 133 (China); Marczak et al., *supra* note 37 (China).

[236] *NETmundial Multistakeholder Statement*, *supra* note 17, and accompanying text.

[237] 2015 GGE Report, *supra* note 9, annex.

[238] *See supra* notes 79, 147, and accompanying text.

[239] *See supra* note 225 and accompanying text.

[240] *See supra* notes 98–104 and accompanying text.

[241] *See* Kenneth W. Abbott, Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter & Duncan Snidal, *The Concept of Legalization*, 54 INT'L ORG. 401, 412–14 (2000).

Where a norm is located institutionally may also influence its prospects for acceptance. For example, one key strategic question facing many norm entrepreneurs is whether they should graft their norms onto existing organizational arrangements or build new ones.[242] Each path has advantages and potential pitfalls. Examples of grafting efforts are already common in cybersecurity. Before it pronounced its own set of norms, the GGE sought to situate its norms for military operations in cyberspace within existing normative regimes in international law.[243] Similarly, when states wanted norms on cybersecurity exports, they turned to the preexisting Wassenaar Arrangement.[244] And, of course, in the Internet governance context, calls persist to shift the relevant norms from their current dispersed multistakeholder locations to the (intergovernmental) ITU framework.[245]

States and others may choose to graft because it is cheaper and easier than starting from scratch and also because doing so offers opportunities to leverage the institution's past success in favor of the norm(s) that they are promoting. Regimes like international humanitarian law and institutions like Wassenaar are known quantities with established track records. Situating cybernorm processes within existing regimes and institutions may give the desired cybernorm greater visibility than a stand-alone campaign. Grafting may also give the new norm an aura of legitimacy that can engender broader acceptance and perhaps even internalization.

Host institutions can impose limitations on grafted norms, however, as the institutions' own organizational processes and cultures come into play and shape norm development. For example, by choosing Wassenaar—a creature of Cold War security politics—to pursue norms on trading in cybersecurity items, the emerging cybernorms favored security interests over economic research and development concerns. Moreover, to the extent that states constitute Wassenaar's membership, views held there on surveillance and privacy were likely different from those that would have emerged from a process involving states *and* civil society groups.[246] Such effects may explain the rising resistance to Wassenaar's norms (and the push for their revision), especially in the United States.[247]

In lieu of grafting, cybernorm entrepreneurs may push for a new institution or stand-alone process. Here, too, we already have several ongoing examples for cybersecurity, including the London Process, Freedom Online Coalition, and ongoing Internet Assigned Numbers Authority transition.[248] Creating entirely new processes has advantages. It allows for tailor-made approaches that can focus exclusively on one or more cybersecurity problems. The specialized focus can draw in experts whose presence can, in turn, improve the norm's articulation or functionality. New processes can bypass constraints of preexisting institutions, whether in terms of their predefined membership or their values. They also avoid competition within a

[242] On grafting, see *supra* note 146 and accompanying text.

[243] *See supra* notes 9, 225, and accompanying text. On states' strategic use of international organizations, see Eneken Tikk-Ringas, *The Implications of Mandates in International Cyber Affairs*, GEO. J. INT'L AFF. 41 (2012).

[244] *See* Wassenaar Arrangement, *supra* note 13.

[245] *See supra* note 81 and accompanying text.

[246] *See* Wassenaar Arrangement, *supra* note 13.

[247] *See*, *e.g.*, Aliya Sternstein, *This Cyber 'Safeguard' Is Hurting US Defenses*, DEFENSE ONE (Jan. 13, 2016), *at* http://www.defenseone.com/technology/2016/01/cyber-safeguard-hurting-us-defenses/125093/.

[248] *See*, *e.g.*, Freedom Online Coalition, *supra* note 231; *NTIA IANA Functions' Stewardship Transition*, *supra* note 100; Global Conference on CyberSpace, *supra* note 10 (London Process); *see also* AUSTIN ET AL., *supra* note 14 (proposing new cybernorms forum).

preexisting institution over its mission or resource allocation between cybernorms and legacy processes.

Nevertheless, the huge costs in starting up new processes—in terms of time, money, and political will—may contrast poorly with even very imperfect grafting alternatives. Indeed, many entrepreneurs pursuing new cybernorms with new processes have complained of just this problem. We remain in a period of "infinite meetings," with nearly every day witnessing an international conference or gathering dedicated to cybersecurity and norms to govern it.[249] The amount of time and attention required to participate in all these projects simultaneously may eventually lead to fatigue, resulting in the cessation or consolidation of various processes. It may also lead to the exclusion of actors with more modest means, who may lack the capacity to participate in so many forums. Indeed, there are already doubts about the future of norm-cultivation efforts associated with the likes of the Freedom Online Coalition and NETmundial. Thus, no path to cybernorms is easy. Frustrations and dangers are associated with whichever institutional home and norm structure entrepreneurs might choose. But being clear-eyed and strategic about their choices is a good starting point.

Propriety: On what basis do norms shape expectations? Even after cybernorm entrepreneurs decide what groups to target and what regulatory or constitutive norms they desire, questions about propriety remain: how can they best create "oughtness" for those norms? Effective norms might be grounded in law, politics, and an array of culture frameworks, each of which carries different potential risks and rewards.

Both international law and international relations scholars have already explored many of the trade-offs involved in decisions to pursue norms in treaties versus norms in *political commitments*.[250] These differences have clear applications in the cyber context. Treaties, for example, offer credible expectations of future behavior. That is not to say that states do not breach their treaty commitments but rather that treaties tend to have more credibility than other bases for setting expectations.[251] The time, effort, cost, and reputational investments in the treaty-making process, once completed, pull parties to fulfill their commitments. Indeed, most treaties require states to complete domestic legal procedures prior to ratification. That practice reinforces the credibility of the treaty's expectations because domestic actors have had an opportunity to contest or alter the treaty's norms. Domestic acceptance of the norms thus reinforces other states' expectations of the party's future performance.[252]

But the credibility that treaties offer comes at some cost. Treaties can be difficult to achieve since they require two levels of agreement. Governments must first agree, and for cybersecurity such agreement seems unlikely on a broad range of issues (for example, content controls). In

[249] The Stockholm Internet Forum's chair described 2014 as "the year of infinite meetings," but the pace has continued unabated. *See* Anna-Karin Hatt, Minister for Information Technology & Energy, Swedish Ministry of Enterprise, Energy, and Communications, Opening Address at the Stockholm Internet Forum (May 27, 2014), *at* http://www.stockholminternetforum.se/the-opening-address-by-anna-karin-hatt/.

[250] *See*, *e.g.*, Duncan B. Hollis & Joshua J. Newcomer, *'Political' Commitments and the Constitution*, 49 VA. J. INT'L L. 507 (2009); Kal Raustiala, *Form and Substance in International Agreements*, 99 AJIL 581, 613 (2005); Abbott et al., *supra* note 241; Charles Lipson, *Why Are Some International Agreements Informal?*, 45 INT'L ORG. 495 (1991). Other scholarship describes the trade-offs via levels of uncertainty, risks of opportunistic behavior, and diversity in interests and preferences. Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54 INT'L ORG. 421 (2000).

[251] Lipson, *supra* note 250, at 511.

[252] John K. Setear, *Treaties, Custom, Iteration, and Public Choice*, 5 CHI. J. INT'L L. 715, 725–27 (2005).

addition, even when intergovernmental agreement might be possible, domestic actors often have an opportunity to approve or reject the treaty's contents. And after a treaty has entered into force, its norms are often difficult to amend if circumstances require later adjustment; treaty amendments usually require the same level of approval as the original treaty, making the treaty process a slow one.[253]

In contrast to treaties, pursuing norms through politics—in particular, political commitments—allows for a more flexible approach to the construction and diffusion of cybernorms. As a general rule, political commitments require no domestic processes for approval.[254] Not only can political commitments be reached quickly and simply among willing actors, but those actors are not limited to states—an important consideration in a multistakeholder world like cyberspace.[255] That flexibility continues after formation since political commitments can generally be adjusted easily or even, if necessary, be rejected by terminating or withdrawing the commitment.[256] Although states and others have been less than explicit in their rationales, some of these factors likely explain the current proliferation of political-cybernorm projects today.

Situating cybernorm processes within political commitments is not, however, without downsides. Political commitments tend to communicate less strong or less intense expectations of future behavior than a treaty would.[257] Adoption of a cybernorm via a political commitment comes with fewer assurances that states (or other actors) will internalize its contents. For example, there are widespread concerns that China's political commitment not to engage in cyberespionage for commercial advantage is mere lip service.[258] Of course, as we discuss, even lip service may have normative effects, but these effects are obviously weaker than more institutionalized and internalized alternatives.

Confidentiality is another mixed feature of political commitments. One of the touted benefits of political commitments is that they can be kept secret if desired.[259] Secrecy would not, of course, disrupt the ability of those sharing the secret to adopt or internalize its norms. But secrecy can pose problems for broader norm cascades or cycles in much the same way that secrecy and attribution problems complicate cybersecurity itself.[260] Actors cannot internalize norms they cannot know. Thus, cybernorm entrepreneurs face the trade-offs between the *ex ante* credibility and domestic legal support of treaties and the *ex post* flexibility and confidentiality of political commitments.[261] They need to strategize accordingly.

[253] International relations scholars have suggested that treaties are thus less flexible than political commitments. Lipson, *supra* note 250, at 500. Although sometimes true, modern treaties (for example, multilateral environmental agreements) may contain built-in adjustment mechanisms to accommodate new facts, scientific developments, or agreements. *See* Jutta Brunnée, *Treaty Amendments*, *in* THE OXFORD GUIDE TO TREATIES 347 (Duncan B. Hollis ed., 2012); Laurence R. Helfer, *Nonconsensual International Lawmaking*, 2008 U. ILL. L. REV. 71, 75 (2008).

[254] Hollis & Newcomer, *supra* note 250, at 512, 526.

[255] For a domestic analysis, see Jacob E. Gersen & Eric A. Posner, *Soft Law: Lessons from Congressional Practice*, 61 STAN. L. REV. 573 (2008).

[256] Hollis & Newcomer, *supra* note 250, at 526. Treaties do, however, regularly contain exit provisions. Laurence R. Helfer, *Terminating Treaties*, *in* THE OXFORD GUIDE TO TREATIES, *supra* note 253, at 634.

[257] Lipson, *supra* note 250, at 511.

[258] *See*, *e.g.*, David J Lynch & Geoff Dyer, *Chinese Hacking of US Companies Declines*, FINANCIAL TIMES (Apr. 13, 2016), *at* http://on.ft.com/1oXtfnm.

[259] Hollis & Newcomer, *supra* note 250, at 526.

[260] *See supra* notes 196–203 and accompanying text.

[261] Raustiala, *supra* note 250, at 592.

Of course, treaties and political commitments are only two of the many bases on which to develop cybernorms. Since customary international law involves a habitual state practice accepted as law, it can, as such, often encapsulate norms for states.[262] Custom has the advantage of emerging without the explicit consent of its subjects, thereby avoiding the need for multiple levels of agreement as required by treaty making. The existence and meaning of customary norms can be hard to discern, however, amid the noise of international relations. This indeterminacy leaves open the possibility of incomplete intersubjectivity, wherein members of the group do not completely converge around a norm's justification and meaning. The capacity for states and others to act anonymously in cyberspace creates another problem for custom. If the most skilled and experienced actors readily disguise their behavior, the content of customary cybernorms may come from the practice of actors who cannot anonymize their activity, either for institutional reasons or because they have less experience and skill. The best practitioners may not, in effect, be the source of the best practices that can be identified or that are adopted. We might imagine, for example, a norm emerging about appropriate encryption standards that specifies an encryption level insufficient to protect data, given the (hidden) expertise of more skilled states or other actors (for example, hackers, cybercriminals).

Domestic law may also serve as a basis for cybernorms.[263] Domestic law offers some of the same credibility benefits as treaties and also the possibility of criminal, civil, and administrative legal enforcement mechanisms that can drive the norm's adoption and distribution within the domestic setting. But domestic law also comes with drawbacks. For many states, passing new laws can be logistically difficult, as witnessed by the recent multiyear effort to devise the U.S. Cybersecurity Information Sharing Act.[264] And, of course, domestic laws are limited geographically to the state's jurisdictional (usually territorial) boundaries. This limitation may create problems for domestic law as a tool for managing global cyber-insecurities if different legislating states seek to codify different cybernorms. These difficulties, among others, help explain why global policy experts are choosing to focus now on the international stage, including new normative efforts to improve mutual legal assistance among states on cybersecurity challenges.[265]

Cultural, particularly professional, norms provide another basis for cybernorm propriety. Such norms already exist in various manifestations, whether Silicon Valley's support for encryption or understandings of proper cybersecurity among the professionals who practice it.[266] Like customary international law, cultural cybernorms do not require the explicit consent or agreement of group members. Moreover, successful cybernorms can become so embedded within a culture that their performance becomes automatic, providing those norms greater reliability and stability. That reliability and stability can even extend beyond the particular cultural group that adopts the norm. For example, professional standards instruct members of a profession on what to do and not do, but they also alert those who interact with professionals what

[262] *See supra* note 126 and accompanying text.

[263] *See supra* note 110 and accompanying text.

[264] *See* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N (2015).

[265] Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SECURITY J. (Jan. 28, 2015), *at* http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/.

[266] *See supra* notes 142–44 (re: encryption), 171 (re: cybersecurity professionals).

behaviors to expect. Just as patients expect their doctors to adhere to the standards of the profession, so, too, may businesses expect an ICT provider to adhere to its own association's standards. As a result, the cultural norms of a profession engaged in cybersecurity may become shared expectations across multiple culture groups.

This last point is worth emphasizing. The reality of modern cybersecurity belies the existence of any single cultural system. Thus, pursuing cultural cybernorms risks creating the same islands of normativity around specific cyber issues. The existence of such islands may be perfectly functional. Many cybersecurity problems, particularly technical ones, do not require broad agreement beyond the technologists involved. Broader issues touching more types of actors, however, might see conflict among the cultural norms of different parties that have stakes in the issue.

Of course, cybernorm entrepreneurs may choose to orient their projects in multiple bases of propriety simultaneously. For example, even as the United States has pursued new information-sharing norms within its domestic law, it has also (successfully) pursued information-sharing as a global "peacetime" norm at the GGE.[267] Pursuing multiple pathways simultaneously may increase the prospects for norm adoption in at least one context, but the dynamic nature of different norm processes in different contexts could also produce competing or conflicting versions of the norm.

In lieu of simultaneous projects, cybernorm entrepreneurs may consider sequencing as a strategy to ease actors into norm acceptance.[268] They could begin by pursuing norms on the simplest basis to achieve—say, a political commitment among a group of like-minded actors—then move to internalize the norms further by attempting codification in law, ultimately producing culturally based behavioral expectations. Or entrepreneurs could choose to focus on cultural values first and use that as a basis for norm construction via a political commitment or a treaty at a later date. Such choices will depend on desired goals and the given context. As Goodman and Jinks emphasize, there are no universal rules here.[269] But sequencing of this kind follows the well-established logic of confidence-building measures: start with the low-hanging fruit where agreement is easiest.[270] Then, as habits of cooperation build up, expand the range of agreement either horizontally, to more parties, or vertically, to deeper, more contested norm issues. Again, there is no recipe for balancing these trade-offs, but awareness of them can make for better strategies.

Collective expectations: How much intersubjectivity to pursue? Unlike the previous three ingredients—identity, behavior, and propriety—most cybernorm entrepreneurs have a clear first choice for setting collective expectations: full internalization. Cybernorm entrepreneurs hope that their norms can achieve the deep-seated, intersubjective status that many existing norms already enjoy. Cyberspace's attribution issues may make this tricky, however, since they hinder a group's ability to police norm observance by its members. Actors may hide their behavior from others, and false flags may cloud issues of responsibility (meaning that the alleged norm

[267] Consolidated Appropriations Act, 2016, *supra* note 264; Grigsby, *supra* note 148; 2015 GGE Report, *supra* note 9, para. 13(j).

[268] GOODMAN & JINKS, *supra* note 155, at 180.

[269] *Id.* at 180–82.

[270] This appears to be the Organization for Security and Co-operation in Europe's strategy. *See* Organization for Security and Co-operation in Europe, Permanent Council, *Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1106 (Dec. 3, 2013), *at* http://www.osce.org/pc/109168.

violator may not actually bear responsibility for the violation). Fully internalized norms can be particularly valuable in such situations because actors will be self-motivated and will continue to "do the right thing" whether or not their behavior is observable by others.

Strategic issues arise when full internalization is not an available option. Differing values and interests among members of the targeted community may preclude complete intersubjective concurrence. In such cases, cybernorm entrepreneurs may have to settle for insincere norms or incompletely theorized ones.[271] At first glance, incompletely theorized norms appear preferable to norms that are merely given lip service. After all, the incompletely theorized norms result in agreement not only on the norm's expression but on the behavioral expectations that it contains. As a result, the reliability of those expectations is greater than cases of insincere conformity, where actors may conform in a limited or inconsistent manner, if at all. Incompletely theorized norms achieve this result by setting aside the inconsistent (and perhaps irreconcilable) goals, values, and interests that preclude the norm's full internalization. In heterogeneous contexts like those presented by cybersecurity, incompletely theorized norms can be the best available option.

It would be a mistake, however, to treat incompletely theorized norms as preferable in all cases. They remain—to paraphrase Philip Allott's famous description of treaties—"disagreement[s] reduced to writing."[272] These norms represent compromises in situations where its subjects do not agree on *why* the norm exists. That lack of agreement may not matter in many cases of cybersecurity (particularly those requiring coordination of actors around some common norm like TCP/IP). But when the norm emerges in a collective-action context, these fundamental differences may not remain hidden for long. If multiple actors continually pursue a closer alignment of the norm to their basic goals, values, or interests, we can expect that incompletely theorized norms may become a locus of constant discord.

Norms subject to insincere conformity, by contrast, do not necessarily result from compromise but may rather take on the character of a Pyrrhic victory, depending on the depth and type of insincerity. Norm entrepreneurs are able to declare success even as some of those adopting the norm intend to observe it as little as possible. Such behavior might suggest lower prospects for full internalization. Indeed, insincere conformers may be resentful of the conditions that led to their adoption of the norm (such as acts of coercion), which may lead them to reject the norm as soon as possible. For cybersecurity, in particular, attribution issues may also facilitate this behavior, thereby allowing actors to publicly adopt the norm but to secretly act contrary to its expectations. Hence, many in the cybersecurity community continue to look for hard evidence of an actual decrease in acts of commercial cyberespionage originating in China.[273] Norms subject to insincere conformity thus risk normalizing and legitimizing hypocrisy.[274]

Still, insincere conformity may be preferable to no norm at all since it has the potential, over time, to lead to some internalization within the community. Looking at China again, even if it signed onto a ban on commercial cyberespionage without any intention of following through, it now faces a choice between doubling down on its hypocrisy (that is, continuing to

[271] *See supra* notes 120–22 (re: insincere conformity), 123–125 (re: incompletely theorized agreements), and accompanying text. Of course, actors could try to pursue both simultaneously.

[272] Philip Allott, *The Concept of International Law*, 10 EUR. J. INT'L L. 31, 43 (1999).

[273] *See* Iasiello, *supra* note 120.

[274] *See* Henry Farrell & Martha Finnemore, *The End of Hypocrisy: American Foreign Policy in the Age of Leaks*, FOREIGN AFF., Nov./Dec. 2013, at 22.

deny it engages in cyberespionage *and* insisting it is living up to the norm) or shifting its behavior to accord with that norm in some respects. The arrests of the purported perpetrators of the OPM hack suggest that China is taking the latter course, as do recent reports of a drop in commercial cyberespionage.[275] Similarly, even if China (or Russia or the United States) signed off on some or all GGE norms insincerely, the GGE process would still continue creating opportunities for this organizational platform to improve these norms' institutionalization and internalization.

For some entrepreneurs, norms of insincere conformity may even be preferable to incompletely theorized norms. An incompletely theorized cybernorm only papers over irreconcilable goals or values, giving group members an incentive to continue to fight over the norm's interpretation and evolution. By contrast, insincerely adopted norms are less likely to be openly contested. After all, the whole point of going through the motions of adoption is to gain benefits from the appearance of accepting the norm; open rejection would defeat the purpose. Insincere conformity can have unintended consequences, however. Over time, norms subject to insincere conformity can gradually shift the underlying goals, values, and interests of actors originally (but quietly) hostile to its contents. Thus, insincere conformity can evolve into a complete victory in ways that are unlikely if the entrepreneur pursues an incompletely theorized norm.

Selecting Normative Tools: Trade-Offs in Incentives, Persuasion, and Socialization

Having chosen a context and having framed the norm in terms of identity, behavior, propriety, and collective expectations, cybernorm entrepreneurs must decide what tools they will use to promote their norms' adoption and diffusion. Do they employ incentives, persuasion, socialization, or some combination thereof to achieve success? As with other choices, the decisions taken involve weighing consequences and trade-offs.

The literature on using incentives in international relations is extensive. For many analysts, incentives alone—in the form of coercion or inducements—control behavior, at least among states.[276] On this view, crafting the proper package of coercive measures or inducements is the best strategy to ensure norm observance at tolerable, if not perfect, levels. Several limits on this tool are obvious. One is that incentives may not be an option for poor, weak actors; incentives are a tool of the rich and strong. Another is that incentives often must be maintained for long periods of time.[277] Simply put, does the entrepreneur have the will and resources to keep up the incentives indefinitely or long enough for socialization processes to take hold? If the answer is no, termination of incentives can lead to a backlash and rejection of a norm, perhaps leaving promoters in a situation worse than where they started.

[275] *See* Nakashima, *supra* note 64; Iasiello, *supra* note 120. *But see* Gady, *supra* note 120.

[276] *See* GOODMAN & JINKS, *supra* note 155, at 23.

[277] *Id.* at 167. The tolerability calculus may depend on what Goodman and Jinks call "targeting capacity"—namely, the "capacity to direct pressure against specific actors." *Id.* at 183. Incentives do not work well in poor targeting-capacity cases since targeted actors can avoid the coercive costs or pass them off to other actors. The attribution problem often complicates targeting for cybersecurity. Only when the actor's identity may be determined can incentives lead to norms. The threat of cybersanctions against specific Chinese officials, for example, may explain their adherence to the cyberespionage norm.

Persuasion holds out the promise of fuller internalization and may be assisted by incentives.[278] The same framing and linking used to define the context for cybernorms may be deployed to persuade actors of the norm's validity or appropriateness, as discussed earlier. Persuasion can be difficult, however, and comes with its own risks. Persuading actors with very different value systems is always difficult (unless the resulting norm is incompletely theorized), and the Internet is a paradigmatic example of a policy space populated by actors with different goals and values. Moreover, persuasion is unlikely to work on "bad actors" such as cybercriminals, who have no interest in conforming to social norms. Persuasion is also uneven across groups, creating ongoing tensions and conflict; for example, some hacktivists may become convinced of the legal or cultural propriety of limiting or forgoing hacking, but many remain unpersuaded.

Persuasion can also have a "norm capture" problem for entrepreneurs.[279] The Framework Convention on Tobacco Control is a prominent example of this phenomenon.[280] In the final stages of the negotiations, the original alliance of 180 NGOs—which pushed for the convention in the first place—were excluded by states and lost control of the substantive agenda.[281] This phenomenon can apply even to powerful actors. The United States successfully persuaded members of the UN GGE to accept a norm making states responsible for the cyber-operations of their proxies, but if Russia and perhaps China have their way, the norm's emphasis could shift. Rather than targeting proxies and states that host them (the U.S. goal as entrepreneur), the Russian and Chinese norm would focus on accusers and require that allegations of state support for proxies be made "responsibly," thus shifting the norm's goals entirely.[282]

Actors may learn the behavioral expectations of their community on their own, but the process can often be aided by entrepreneurs using tools of social influence. Naming and shaming conduct deemed inappropriate by the community is one tool that can lead violators to adjust their behavior while at the same time reinforcing the norm within the group.[283] In cybersecurity, companies whose hardware or software contains a vulnerability are regularly named and shamed to do something to patch it.[284] Groups like Anonymous meanwhile engage in *doxing*—a particular form of naming and shaming—in which personal details of perceived norm violators are released online.[285]

Socialization's success depends in part on the violator's capacity to conform and on the "tightness" of the group identity in question. The smaller and more connected the group, the more that shaming can socialize behavior (hence, it is often most effective within families). Conversely, the social pressures of larger and more disparate groups may not be enough to

[278] *Id.*

[279] *See supra* notes 161–64 and accompanying text.

[280] WHO Framework Convention on Tobacco Control, May 21, 2003, 2302 UNTS 166.

[281] Kal Raustiala, *NGOs in International Treaty-Making*, *in* THE OXFORD GUIDE TO TREATIES, *supra* note 253, at 150, 168–69.

[282] *See* 2015 GGE Report, *supra* note 9, para. 13(f); Grigsby, *supra* note 148.

[283] *See supra* note 172 and accompanying text.

[284] This is true whether or not the company intended it. *See*, *e.g.*, Thomas Fox-Brewster, *Thunderstrike 2: Remote Attacks Can Now Install Super Stealth 'Firmworm' Backdoors on Apple Macs*, FORBES (Aug. 3, 2015), *at* http://www.forbes.com/sites/thomasbrewster/; Seth Rosenblatt, *Lenovo's Superfish Security Snafu Blows Up in Its Face*, C/NET (Feb. 20, 2015), *at* http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/.

[285] Cole Stryker, *The Problem with Public Shaming*, NATION (April 24, 2013), *at* https://www.thenation.com/article/problem-public-shaming/.

change the violator's behavior. Violators may simply decide the group identity is not worth having and exit from the group entirely. The practice of doxing can lead its targets to issue apologies or adjust their behavior, but it can also backfire when the community itself largely rejects the appropriateness of naming and shaming. Members of the group may even defend the violator's behavior against doxers, putting the norm's existence into question.

Capacity building, whether through communication networks, technical assistance, or training, constitutes a less coercive mechanism for socialization that often works through teaching and empowering. Communication platforms like the Cybercrime Convention's 24/7 network allow users to share information and coordinate action on cybercrimes and thereby to develop shared views on desired behavior.[286] Repeated interactions structured to pursue normative goals may lay the basis for a new community that, over time, may come to strengthen norms. Technical assistance may also embed norms within training curricula and may showcase best practices for actors to mimic. The German and U.S. governments, for example, fund a three-week Program on Cyber Security Studies, which gathers government officials and experts from nearly fifty countries to train on a whole range of cybersecurity topics.[287] The contents of that course offer a reference for its students on what behavior is appropriate or inappropriate in cyberspace, not to mention giving them a new community, going forward, with which to identify.

Soft as that German-U.S. exercise of power is, it is worth remembering that capacity building is ultimately an effort to exercise power over those in need of networks, assistance, or training. It matters who exercises that power. Different capacity builders will promote different norms. U.S. efforts through the U.S. Telecommunications Training Institute, for example, contrast with the norms advanced by China in its annual World Internet Conference, with the latter in the past pushing the propriety of complete sovereign control over ICTs.[288]

Our catalog of risks and rewards associated with strategic social construction of cybernorms comes with a few significant caveats. First, our categories are artificially tidy ideal types. We have chosen to isolate particular contexts, ingredients, and tools to illustrate their significance and potential consequences. Real-world international relations are not so simple. Many of these concepts are not easily disentangled one from another. Issues like identity are entirely intertwined with culture, just as socialization's naming-and-shaming stigma can be tied up with material incentives.

Second, entrepreneurs must continue to account for the dynamic character of cybernorms. The success (or failure) of their choices can engender (or foreclose) other options in the future. Actors must expect unforeseen circumstances and evolution, which are inherent in the normative environment. Thus, the strategic choices that we have illustrated above are not one-time decisions but are part of a *process of decision making*. Actors must continuously evaluate (or reevaluate) their choices and be ready to adjust to the current environment.

Finally, the cybernorms governing different aspects of cybersecurity are both diverse and interdependent, which creates challenges for norm promoters. Changing cybernorms on

[286] Budapest Convention, *supra* note 11, Art. 35.

[287] George C. Marshall European Center for Security Studies, *Program on Cyber Security Studies (PCSS)*, *at* http://www.marshallcenter.org/mcpublicweb/en/nav-main-wwd-res-courses-pcss-en.html.

[288] United States Telecommunications Training Institute, *supra* note 171; Samm Sacks, *Cybersecurity Won't Be the Biggest Deal at China's World Internet Conference*, FORTUNE (Dec. 15, 2015), *at* http://fortune.com/2015/12/15/cybersecurity-china-world-internet-conference/.

encryption can affect norms governing cybercriminals, just as norms on cyberespionage may affect norms for zero-day markets. Thus, even as we call on actors to focus more on norm processes, they must do so systemically, with an eye to the larger norm landscape. Just as individual cybernorm processes involve trade-offs, so, too, will larger projects seeking to construct sets or systems of cybernorms. Further study of the precise nature and contours of those trade-offs may thus further improve the prospects for stabilizing cybersecurity.

V. Conclusion

On December 23, 2015, the UN General Assembly unanimously adopted a resolution requesting that the UN secretary-general establish a new Group of Governmental Experts on Information Security to study (with a view to promoting) "norms, rules and principles of responsible behaviour of states, confidence-building measures and capacity-building."[289] But how will the new GGE proceed with this task? The previous GGE chose to emphasize content, working to negotiate agreement on a series of specific expectations for appropriate state behavior in the ICT environment.[290] In doing so, the GGE typified the dominant approach to cybernorms. From the *Tallinn Manual* to the G-20 statement denouncing commercial cyberespionage, states and other stakeholders have focused on negotiating language delineating the behavior that they want to see (or not see) in some future cyberspace.

Our article offers a different lens for understanding cybernorms. We share the sense of urgency that surrounds current norm-promotion projects; the scope and scale of the economic, privacy, and national security stakes are too great to ignore. But an approach that negotiates only content and ignores norm construction and evolution processes will have limited effects. Promoters of cybernorms are not working with a blank slate. Today, cybernorms exist in various states of development and diffusion, whether one sorts them according to *identity* (which group or community they target), *behavior* (how they regulate), *propriety* (the basis or reason on which they delineate behavior as proper or improper), or *collective expectations* (the extent of intersubjectivity and internalization that norms receive).

Our real challenge lies, however, in overcoming the view of cybernorms as the fixed products of negotiation, locked-in agreements that can settle expectations. The value of cybernorms comes in the processes by which they operate as much as the contents (or products) that such processes generate. Indeed, we argue that, in important ways, the process *is* the product when it comes to cybernorms. Constructing robust processes through which cybernorms can develop and evolve is essential for cybersecurity. Social science research can be helpful in understanding what such processes might look like and how they work, and we have cataloged some obvious lessons here. We know, for example, that cybernorms can be fostered using various tools of influence, including incentives, persuasion, and socialization. We also know that cybernorms, like all norms, will be dynamic; they will evolve over time through repeated interactions among those involved in the norms' construction and use. Cybernorms are also both diverse and interwoven—meaning construction and change in one norm may influence others in the broader cybersecurity space.

[289] GA Res. 70/237, para. 5 (Dec. 30, 2015). The resolution contemplates the GGE reporting back to the General Assembly in 2017.

[290] 2015 GGE Report, *supra* note 9, para. 13. The new GGE will expand its membership from twenty to twenty-five governmental experts.

Novel though cyberspace may be in some ways, we are convinced that important lessons can be learned from other norm-cultivation efforts in other regulatory domains. Norms elsewhere have had to deal with rapidly changing situations and technologies, with a similar global scope and scale, and with problems of secrecy that may complicate social learning and shared expectations. From the regulatory role of code to the multistakeholder model of governance, analogues to cyberspace exist that affirm the utility of bringing the lessons of other norm processes into the cyber environment. We believe our process-centered approach holds out the promise of more informed, if not more successful, construction of cybernorms by states and other stakeholders who approach these issues strategically.

Beyond our article's import for practitioners, our interdisciplinary efforts offer insights that may benefit both the international relations and international law disciplines. For international relations, our article offers a detailed elaboration of strategic social-construction challenges involved in constructing the "who should do what" core of any norm. Research on norms in international relations has often treated the construction of desired norms as unproblematic. For norm entrepreneurs in the much researched fields of civil and political rights, norms like "states should not torture" were relatively obvious. In cybersecurity, by contrast, who should do what to achieve shared goals is far less clear. Our article also highlights norm characteristics such as incomplete theorization and insincere conformity that are essential to political compromise but that also may contain seeds of instability. In highlighting these active construction processes, we hope to advance understandings of norm dynamics more generally by exploring the problem of cybernorm cultivation in a heterogeneous contextual and normative environment.

For international lawyers, our analysis offers an expanded view of law's functions. International lawyers (and lawyers generally) have tended to conceive of regulatory issues only in legal terms. They generally presume the normative force of laws. But problems of compliance in international law have complicated this presumption, leading to new efforts to catalog when law works (whether in terms of compliance patterns or, more broadly, law's effectiveness) and to the study of alternative regulatory models, including soft law and political commitments.[291] For all the attention to diverse regime-design possibilities, however, international lawyers have not devoted the same attention to understanding the processes by which regimes work and create desired effects.[292] How does international law (or soft law or a political commitment) come to embody norms for states and other subjects of international law? Our effort examines precisely this question. And although current efforts focus on nonlegal cyber options, our analysis provides a framework for strategic thinking that encompasses all the outlets and processes through which cybernorms can emerge and evolve.

Preserving cybersecurity is hard. So, it turns out, is constructing cybernorms. Actors may have goals that they want ICTs to serve, but goals are not norms. Goals, by themselves, do not

[291] *See*, *e.g.*, ANDREW GUZMAN & TIM MEYER, GOLDILOCKS GLOBALISM: THE RISE OF SOFT LAW IN INTERNATIONAL GOVERNANCE (2015); Chris Brummer, *Why Soft Law Dominates International Finance—and Not Trade,* 13 J. INT'L ECON. L. 623 (2010); COMMITMENT AND COMPLIANCE: THE ROLE OF NON-BINDING NORMS IN THE INTERNATIONAL LEGAL SYSTEM (Dinah Shelton ed., 2000).

[292] This is not to say that international lawyers have ignored this issue; several *have* done significant work on international law's social processes. *E.g.*, Koh, *supra* note 133; GOODMAN & JINKS, *supra* note 155. Moreover, global administrative law has emphasized thinking more about how processes and other administrative tools may improve global governance. *See*, *e.g.*, Benedict Kingsbury, Nico Krisch & Richard Stewart, *The Emergence of Global Administrative Law*, LAW & CONTEMP. PROB., Summer 2005, at 15.

tell us who should do what to realize the goal. This is an essential function of norms: they tell us who should do what to achieve goals. Desired outcomes remain in the ether until there are norms (among other instruments) that spell out social expectations for the behavior that might achieve them. How these constructions come into being can be complicated, but neither cyberspace nor its norms are so impenetrable that actors should ignore the various contexts, ingredients, and process tools involved. On the contrary, understanding the actual processes by which cybernorms form, diffuse, and evolve is likely to influence the future shape of cybersecurity as much as the aspirational goals on which actors may agree. By bridging this gap between goals for cybersecurity and the processes that might achieve them, our article opens up avenues for dialogue and further research on norms generally. If successful, these processes themselves can help ensure cyberspace remains accessible, open, stable, and secure.