CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

# CYBERSECURITY AND THE CONCEPT OF NORMS

MARTHA FINNEMORE | NOVEMBER 30, 2017

Calls for norms to secure and stabilize cyberspace have become ubiquitous.[1] These appeals often offer detailed knowledge of cybersecurity but rarely say much conceptually about norms themselves—what they are, how they work, how they spread, and why anyone might prefer them to other policy instruments. As a result, policy discussions and media coverage often apply the term to policy instruments that are not, in fact, norms. Such conflations are understandable, but they can create unnecessary confusion and detract from the norm construction process. Relevant academic literature describes the basic features of the concept of norms and how they work, while also drawing lessons from other policy arenas where norms have, or have not, been used successfully.

## WHAT IS (AND IS NOT) A NORM?

According to a now standard definition, a norm is "a collective expectation for the proper behavior of actors with a given identity."[2] Several features of this definition merit discussion. First, norms are *shared* beliefs held within a community. Something is not a norm just because someone says so; a norm exists only when some relevant group agrees with and holds particular beliefs about expected behavior. Consequently, simply solving the puzzle of what substantive normative prescriptions might address a given cybersecurity problem and announcing this to the world does not create a norm. Others need to buy in and recognize that the norm's behavioral prescriptions apply to them (or to other actors who can be held to account). The U.S. government preaching that commercial cyber espionage is bad did not create a norm against cyber espionage. Only when China, the UK, and other G20 countries signed on did a norm start to take shape. Individuals do not need to like a norm to recognize that its expectations are widely shared, and people do not need to like a norm to feel the pull of its behavioral prescriptions. Most people would not choose to wear neckties or high heels but do so when the occasion demands it. Similarly, states, regulatory bodies, firms, and other actors may chafe at a norm's behavioral prescriptions but conform anyway because they want to maintain their standing in the group and/or because they value the group's goals.

Second, the pull to conform to a norm arises from its being shared within a group with which relevant actors identify. For example, states may not be enthusiastic about every feature of the UN Group of Governmental Experts' output, but many, particularly Western, states feel more pressure to conform to those norms than those promulgated by the Shanghai Cooperation Organization, because they identify with the UN and feel some pull from its processes. This identity component of norms has consequences for norm promulgation strategies. Savvy entrepreneurs can play upon

## ABOUT THE AUTHOR

**Martha Finnemore** *is a nonresident scholar with the Cyber Policy Initiative at the Carnegie Endowment for International Peace. She is also a professor of political science and international affairs at George Washington University in Washington, DC. Her research focuses on global governance, international organizations, ethics, and social theory.*

actors' desires for a good reputation or for membership in a select group, arguing that states (or firms) deemed good or responsible will follow a given norm. Early adoption by these states (or firms) adds credibility and compliance pull to the norm. In this way, widespread adoption of the National Institute of Standards and Technology's voluntary cybersecurity framework, which includes an array of norms, helped actors signal their intentions and build trust in supply chains (and with governments).

## HOW ARE NORMS RELATED TO OTHER POLICY INSTRUMENTS?

Norms are different from and yet are tied to related concepts such as principles or laws. Broadly speaking, principles are "statements of fact, causation, or rectitude" and guide action in a variety of ways.[3] Often, they articulate a goal or vision of what a group wants to achieve. This is useful in that agreement on what a group wants to accomplish can help coordinate activity, although articulating shared principles can be difficult. For example, the notion of protecting human rights online might be a guiding goal or principle, but forging a shared belief in this idea can be challenging, even among states that have signed on to the international community's core human rights instruments (as virtually all states have done).

In contrast to norms, however, principles are often silent or imprecise about which actors should perform which behaviors to achieve a stated goal. Principles may be stated in the passive voice or may describe obligations vaguely. Norms explicitly link specific actors to desirable behavior. If a principle clearly distributes labor and assigns responsibilities, and if those understandings are widely shared by relevant actors, that principle is a norm. If not, it is merely a principle (or goal, or vision, or something else).[4] For example, the claim that information ought to be free might be a principle, but it is not a norm.

Pursuing agreement on principles, as opposed to norms, may be politically attractive precisely because it allows some fudging about behavioral obligations. Articulating specific obligations for specific actors (that is, articulating norms) invites scrutiny and claims of accountability in ways that principles do not. For that reason, constructing norms may be more controversial. Of course, this is also why norms can be more valuable as policy tools. By clarifying responsibilities and who should do what, norms create obligations for identifiable actors and trigger more active accountability than principles do.

Laws are another prominent policy instrument at work in cyberspace. Like principles, laws often work alongside norms to achieve policy goals, but laws are distinct from norms in important ways. For one thing, norms are broader than laws. Notions of proper behavior can have many sources, notably culture, and a variety of cultures intersect in cyberspace. The cultures of Silicon Valley tech firms differ markedly from those at U.S. Cyber Command or the National Security Agency, for example; this can create norm and value clashes, as well as legal disputes, around issues like front and back doors in software. It is worth noting that many powerful social norms—for example, those that indicate what constitutes good software—have little or no legal standing.

At the same time, laws are not entirely autonomous from norms; most forms of law are bolstered by a strong element of normativity. Indeed, many laws aim to create norms by using the legitimacy of law to define shared expectations. There are collective expectations in most states to follow the law, which often performs the important function of spelling out who should do what, a feature of norms. Not every law enjoys broad normative support—as intellectual property lawyers who battle social norms on file sharing understand well—but most laws do. For that reason, one common goal of norm promoters is to construct ties to law that strengthen and refine the behavioral expectations of a given norm.

For example, many professional norms in cyberspace began as best practices (or norms) but have, over time, been written into law in various ways. Not all norms have become legalized, however. Professional norms are often spread through training and socialization efforts. The U.S. Telecommunications Training Institute and capacity-building efforts more broadly train government and regulatory officials from around the world in ways to manage cyber challenges, and in doing so, spread norms. They aim to shape expectations and behavior not through law or enforcement and coercion, but by tapping into participants' professionalism and disposition to share the expectations about proper performance in their professions.

The attraction of writing norms into formal laws, particularly domestic laws, is that the coercive power of the state can backstop expectations and compel compliance. This can, indeed, be a powerful tactic particularly when good mechanisms exist to bring suit and compel enforcement. Liability law is one potentially striking example. However, law's power to create norm-conforming behavior depends heavily on the nature of the domestic legal and political system in question. Formalizing norms in law secures greater compliance and enforcement in some systems than others.

Tying norms to law is thus not a silver bullet for a compliance problem, particularly for norms among states. Human rights advocates have been trying for decades to hold states' feet to the fire and enforce a wide range of international human rights obligations that governments have formally agreed to but refuse to implement. (Recall that Saudi Arabia is a signatory to the Convention on the Elimination of All Forms of Discrimination Against Women.) States use reservations to treaties strategically to hedge, create ambiguity, and duck accountability under such laws. Theoretically, reservations that are incompatible with the object and purpose of the treaty are, themselves, illegal, but efforts to point this out to the Saudis have not been particularly successful. Simply writing shared beliefs into law does not always indicate that the beliefs are actually shared or patch over divisions in what is ostensibly a normative consensus.

Part of the current enthusiasm for voluntary norms as a policy tool seems to stem from widespread doubts about the effectiveness of formal treaties in the cyber domain. Many governments, firms, and civil society actors, particularly in the West, see treaty making as far too slow and clunky for this fast-moving policy space, and fears of locking in an undesirable substantive or procedural outcome are widespread in the U.S. government. Norms may offer a better alternative, as they can be created through multiple channels, including political agreements (which require no Senate ratification), and they can be promoted by multiple types of actors—including firms, civil society groups, and states. Norms among regulatory and technical agencies can be particularly important in managing shared threats. The United States and other actors thus see norms as a nimbler, more flexible way to manage mounting cyber threats.

## WHERE DO NORMS COME FROM? HOW DO THEY SPREAD?

Norms can develop in a variety of ways, particularly through habit and entrepreneurship. Some norms emerge spontaneously without any particular actor having any particular intent and then become entrenched through habit. In any group that interacts regularly, norms develop simply through expectations shaped by repeated behavior. Much of the foundational engineering of the internet involves this kind of path-dependent norm development. For example, the widespread preference for using a Simple Network Management Protocol to manage devices on a network arose from repeated use. Policymakers understand this power of unchallenged repetition and often seek to shape it. For instance, the U.S indictment of five Chinese hackers in May 2014 partly aimed to dispel expectations that state-sponsored cyber espionage for commercial advantage is acceptable.[5]

The majority of policy norms, however, are the result of hard work by interested parties, who in the academic literature are called norm entrepreneurs. These may be individuals, like Henry Dunant, founder of the International Committee of the Red Cross, who in 1863 proposed the norms that are now at the heart of the Geneva Conventions. They also may be nongovernmental organizations like Transparency International that promulgate and promote anticorruption standards. Other examples include technology firms that are actively involved in defining and promoting cyber norms, as well as international organizations like the UN or countries like the United States that are busily pushing desired norms on many fronts.

There is now voluminous scholarship on how norms spread (or fail to spread) in various policy domains. There is no magic recipe for success, but there are some clear strategic choices that norm promoters need to consider.

### To Whom Does a Given Norm Apply?

One distinctive feature of digital governance is the diversity of actors and stakeholders involved. This is not simply an issue to be solved by governments. In contrast to the case of nuclear weapons, the production and use of cyber technology is neither owned or monopolized by governments. This creates opportunities to think creatively about where, exactly, cyber norms might be cultivated to best effect and who, exactly, should be their subjects. There are many projects promoting cyber norms that aim to govern state behavior, but even in these cases, there are trade-offs.

One such choice is between the breadth versus the depth of a given norm. It might be easier to develop collective expectations in a smaller, relatively like-minded group (like NATO). One might also be able to develop deeper expectations for more far-reaching coordination in such a group. The risk may be that one ends up with isolated norm silos across the digital landscape. Groups that are not as like-minded may generate different sets of competing norms. Compare, for example, the Freedom Online Coalition's support for free expression online with the Shanghai Cooperation Organization's norms for limiting subversive political speech. Norm adherence is dynamic, and it may be possible to start small and build out the collectivity that shares a norm. This may be part of the logic underlying the 2015 U.S.-China bilateral agreement on cyber espionage for commercial advantage.[6] When powerful or influential actors publicly embrace a norm, this can have spill-over effects and induce others to follow suit (G20 countries, in the espionage example), strengthening the norm that prominent players support.

### How Are Norms Framed and What Do They Say?

The framing of any issue can have a large impact on its success. Much norm promotion is about persuasion, and the persuasiveness of appeals to adopt various norms depends on how they are presented to potential adopters. Who is promoting the norm is part of this framing and its appeal (or lack thereof). Great powers may not always be the most effective leaders for every effort. Victims of cyber attacks (like Estonia in 2007) may have particular legitimacy and stature in promoting some norms.

Where a proposed norm is located institutionally also matters to its future prospects. Grafting new norms onto existing institutions has the advantage of avoiding bureaucratic start-up costs, but it also ties new norms to extant ones, which may shape the former's future development in powerful ways. For example, many have argued that when states chose the Wassenaar Arrangement—a creature born out of Cold War security politics—as the venue to develop norms (and laws) for internet-based surveillance systems, the emerging cyber norms favored security concerns over the needs of researchers and professionals tasked with responding to cyber attacks.[7] The alternative is to push for a new institution or stand-alone process. The Freedom Online Coalition, the London Process, and the NETmundial Initiative are examples of this approach. This allows promoters to focus more squarely on distinctive needs in cyberspace, but such efforts then enjoy none of the resources or legitimacy-related advantages that may come from attachment to extant institutions.

### Why Do Some Norms Succeed When Others Fail?

Constructing new norms is difficult, and failure is always an option. (It may even be the dominant outcome.) Gatekeepers of various kinds may be strategically situated to shut down discussions of new norms or keep them off the agenda. More fundamentally, shared beliefs are dynamic; they change as contexts do, as new problems arise, and as group beliefs and group membership shift. A long-standing historical norm in warfare was the idea that to the victor go the spoils. Over the twentieth century, acceptance of this norm waned among states that stopped recognizing territorial gains made by force of arms. Shared beliefs are rarely settled for all time, but rather are in constant motion; recent events in Crimea suggest that even this long-settled norm against territorial gains by force may be in some state of flux.

That said, several features could contribute to a given norm's success. Influential and widely respected leadership in promotion of a norm can be important in building shared beliefs and encouraging adherence to behavioral prescriptions. These leaders (or entrepreneurs) need not be the most powerful actors. Efforts to ban landmines in the 1990s were led by civil society actors and coordinated by Canada over objections from more powerful states.

This movement succeeded in part precisely because these actors were not perceived to be pursuing a geopolitical agenda. Connections constructed between a new norm and widely accepted existing norms can similarly bolster the attractiveness of a new norm's claims and the likelihood of adoption.

## THE DYNAMIC NATURE OF NORMS: A CHALLENGE AND OPPORTUNITY

Norms are not fixed products of negotiated agreements that set meanings in stone. Part of the utility, and the challenge, of norms is that their meanings are dynamic. Every new application of a norm to a new situation refines understandings of exactly what the norm entails. These accumulations of shared understanding can give norms depth and make them robust, but these processes can also be contested and messy. Contestation of cyber norms is to be expected, particularly because changing technology constantly creates new situations. Constructing robust institutions and processes through which to have these debates is one way to manage these challenges.

*An initial draft of this article was prepared for the Global Commission on the Security of Cyberspace meeting in Munich, Germany, on February 17–19, 2017. The author is grateful to Duncan B. Hollis for his helpful comments on this draft but maintains responsibility for any errors. A much fuller treatment of all these issues can be found in the following co-authored article.*[8]

## NOTES

[1] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly Document A/70/174, July 22, 2015, para. 9–15, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (also known as the *2015 GGE Report*). Please also see Henry Farrell, "Promoting Norms for Cyberspace," Council on Foreign Relations Cyber Brief, April 6, 2015, 2–3; James Andrew Lewis, "Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms," Center for Strategic and International Studies, February 2014, 8–14; and 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*, edited by Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton, Florida: CRC Press, 2013), 233.

[2] Peter J. Katzenstein, ed., *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press, 1996), 5.

[3] Stephen D. Krasner, *International Regimes* (New York: Cornell University Press, 1983), 2.

[4] Michelle Jurkovich, "What Isn't a Norm? Redefining the Conceptual Boundaries in International Relations," (unpublished manuscript on file with author, 2016); Michelle Jurkovich, "Boomerang or Buckshot? Blame Diffusion in International Hunger Advocacy," George Washington University (unpublished PhD dissertation on file with author).

[5] Department of Justice Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," press release, Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[6] "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," the Office of the Press Secretary, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

[7] Internet Freedom and Export Controls: Briefing Before the Comm. on Security and Cooperation in Europe (U.S. Helsinki Commission), 114th Cong. (2016) (remarks by Tim Maurer to committee chaired by Senator Roger F. Wicker, March 3, 2016), http://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls-pub-62961.

[8] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," American Journal of International Law 110 (forthcoming), https://ssrn.com/abstract=2843913.

**CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE**

*The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance the cause of peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.*

*The Carnegie Cyber Policy Initiative focuses on addressing international cyber policy challenges, as cyberspace is increasingly central to international security and diplomacy. The initiative develops and promotes norms and policy recommendations for enhancing international stability and security in cyberspace.*

Carnegie does not take institutional positions on public policy issues; the views represented herein are the author's own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

@CarnegieEndow facebook.com/CarnegieEndowment