A Short Primer on Norms

By Martha Finnemore, George Washington University

Prepared for the Global Commission on the Stability of Cyberspace Inaugural Meeting,
17 February, 2017, Munich

Calls for norms to secure and stabilize cyberspace are ubiquitous now. These appeals are often detailed in their knowledge of cybersecurity but rarely say much about the norm concept, itself - what norms are, how they work, how they spread, why anyone might prefer them to other policy instruments on offer, particularly law. Drawing on the academic norms literature, this memo briefly sketches basic features of the norm concept and how it works, along with lessons we might learn from other policy arenas where norms have been used successfully, or not. 3

What is (and is not) a norm?
According to by-now standard definitions, a norm is a collective expectation for the proper behavior of actors with a given identity. 4 Several features of this merit discussion. First, norms are “collectively held expectations.” They are shared beliefs held within a community. It’s not a norm just because someone says it is; it’s a norm only when some relevant group agrees and also holds these beliefs about expected behavior. Thus, simply solving the puzzle of what substantive normative prescriptions might solve cybersecurity problems 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). US preaching that commercial cyber espionage is bad did not make a norm. Only when China, and then Germany, the UK, and the G20 signed on did the norm start to take shape. We don’t need to like a norm to recognize that its expectations are, indeed, widely shared, and we don’t need to like a norm to feel the pull of its behavioral prescriptions. Most of us would not choose to wear neckties or high heels, but we do so when the occasion demands it. Similarly, states, regulatory bodies, firms, and other actors may chafe a norm’s behavioral prescription but conform because they want to maintain our standing in the group and/or because we value the group’s goals.

Second, normativity and the conformity pull of a norm arises from its being shared within a group with which relevant actors identify. States may not be enthusiastic about every feature of the GGE’s output but many, particularly Western, states feel more pressure to conform to those norms than, for example, those promulgated by the Shanghai Cooperation Organization, because they identify with the UN GGE and want to be seen as “states in good standing” in that group. This identity component of norms has consequences for norm promulgation strategies. Savvy entrepreneurs can play upon actors’ desires for a

3 A much fuller treatment of all these issues can be found in my article with Duncan Hollis, “Constructing Norms for Global Cybersecurity” American Journal of International Law, 110.3 (2016): 425-479 [included in the Additional Reading List]. I am grateful to Hollis for helpful comments on this draft, but responsibility for errors is my own.

good reputation or for membership in a select group when they promulgate norms, arguing that “good” or “responsible” states (or firms) follow the norm. Early adoption by states (or firms) widely perceived to have that reputation (for being good or responsible) adds credibility and compliance pull to the norm. Widespread adoption of NIST’s “voluntary cybersecurity framework” (which includes an array of norms) helped signal intentions and build trust in supply chains (and with governments) in this way.

**How are norms related to other policy instruments like law or principles?**

Policy discussions and media coverage often apply the term “norms” to policy instruments that are not, in fact, norms. The conflations are understandable but can create unnecessary confusion. They also detract from essential tasks in the norm construction process.

*Principles* are “statements of fact, causation, or rectitude”\(^5\) and guide action in a variety of ways. Often, they articulate a goal or vision of what a group wants to achieve. This is useful. Agreement on what it is we want to achieve can help coordinate activity a host of ways, and articulating shared principles can be difficult. For example, “protecting human rights online” might be a guiding goal or a principle but forging a shared belief in this can be challenging even among states that have signed on to the core human rights instruments (which is virtually all states).

Principles are often silent or imprecise, however, about which actors should do which behaviors to achieve the stated goal. In this way, principles differ from norms. Principles may be stated in the passive voice or be vague about who should do what to achieve the shared goal. Norms, by contrast, explicitly link specific actors to desirable behavior. If principles distribute labor and assign responsibility clearly, and if those understandings are widely shared by relevant actors, they are norms. If, by contrast, we see an articulation of goals without assignment of responsibility and specification of expected behavior, those are principles (or goals or visions or something else); they are not norms. “Information wants 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 because it is often easier to achieve precisely because it allows some fudging about behavioral obligations. Articulating specific behavioral obligations for specific actors (i.e., articulating norms) invites scrutiny and accountability claims in a way principles do not. For that reason, constructing norms may be more controversial. Of course, this is also why norms can be more valuable as tools of policy. By clarifying responsibility and who should do what, norms create obligations for identifiable actors and trigger more active accountability politics than vaguer principles usually produce.

*Law* is another prominent policy instrument at work in the cyber arena. Like principles, law often works alongside norms to achieve policy goals, but it is distinct from norms in important ways. Norms are a broader phenomenon than law. Notions of “proper behavior” can have many sources, notably culture, and a variety of cultures intersect in cyberspace. The culture of Silicon Valley tech firms differs markedly from that at Cyber Command or the NSA, for example, and this can create norm and value clashes, as well as legal ones, around issues like front and back doors in software. Many such powerful social norms have little or no legal standing. At the same time, law is not entirely autonomous from norms; most

forms of law have a strong element of normativity that bolsters and strengthens the law. Indeed, one objective of many laws is to create norms by using the legitimacy of law to define shared expectations. Collective expectations in most states include law-following, and law often performs the important functions of spelling out the “who should do what” features of norms. Not every law enjoys broad normative support, as intellectual property lawyers battling social norms about file sharing understand very well, but most do. For that reason, one common goal of norm promoters is to construct ties to law that strengthen and refine behavioral expectations of the norm.

For example, a great many professional norms in the cyber world which began as “best practices” have, over time, been written into law in various ways. Liability concerns over data breaches and law suits, real or potential, have been powerful engines for formalizing in law these normative expectations about what constitutes due diligence and responsible care by firms and technical professionals. Not all professional norms have become legalized, however. Teaching and socialization efforts like that of the US Telecommunications Training Institute (USTTI) or the Program on Cyber Security Studies at the Marshall Center train government and regulatory officials from diverse states around the world in ways to manage cyber challenges, and in so doing, they 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 powerful particularly when good mechanisms exist to bring suit and compel enforcement, as the liability situation suggests. Law’s power to create norm-conforming behavior depends heavily on the nature of the domestic legal and political system, however. Formalizing norms in law buys more compliance and enforcement in some systems than others.

Tying norms to law is not a silver bullet for the compliance problem, however, particularly for norms among nation states. Human rights advocates have been trying for decades to hold states’ feet to the fire and get enforcement of a wide range of international human rights laws and obligations to which governments have formally agreed 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 law. 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 thus does not always indicate shared beliefs or patch cracks in 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. Treaty making is seen by many 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 US government. Norms are may offer a better alternative. Norms can be created through multiple channels including through political agreements (i.e.
no Senate ratification), and at multiple levels of action. Norms among regulatory and technical agencies can be particularly important in managing shared threats. The US and other actors thus see norms as a more nimble and flexible way to manage mounting cyber threats.

*Where do norms come from? How do they spread?*
Norms can develop in a variety of ways. Of particular importance are habit and entrepreneurship. Some norms emerge spontaneously without any particular intent by any particular actor, and become entrenched through habit. In any group that interacts regularly, norms will develop simply through repeated behavior since regularized behavior shapes expectations within the group. Much of the foundational engineering of the Internet involves this kind of path dependent norm development. For example, widespread preference for using Simple Network Management Protocol (SNMP) to manage devices on a network arose from repeated use. Policy makers also understand this power of unchallenged repetition and often seek to shape it. U.S indictment of five Chinese hackers in May 2014 was clearly an effort to disrupt expectations that state-sponsored cyberespionage for commercial advantage is acceptable.

The majority of policy norms, however, are the result of hard work by interested parties who in the academic literature are called *norm entrepreneurs*. Norm entrepreneurs may be individuals, like Henry Dunant, founder of the International Committee of the Red Cross, who in 1863 proposed the norms that are now the heart of the Geneva Conventions. They may be NGOs like Transparency International who promulgate and promote anti-corruption standards. They can be firms, like Microsoft, which is actively involved in the effort to define and promote cybernorms; they can be international organizations, like the UN or nation states like the US, both of whom 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 the norm apply?* One distinctive feature of digital governance is the diversity of actors and stakeholders involved. This is not simply a problem to be solved by governments. Unlike nuclear weapons, governments neither own nor monopolize production and use of this technology. This creates opportunities to think creatively about where, exactly, cybernorms might be cultivated to best effect and who, exactly, should be their subjects. There are a great many cybernorm promotion projects to govern state behavior, but even here there are trade-offs and choices.

One is between what we might think of as “breadth” vs “depth” of the norm. It might be easier to develop collective expectations in a smaller, relatively like-minded group, (for example, NATO). One might also be able to develop deeper expectations for more far-reaching coordination among a like-minded group. The risk may be that one ends up with norm “silos” across the digital landscape. Groups that are not “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 the norm. This may be part of the logic
underlying the US-China agreement on cyberespionage for commercial advantage. When powerful or influential actors publicly embrace a norm, this can have contagion effects and induce others to follow suit (the G-20, in the espionage example) strengthening the norm that prominent players support.

How is the norm “framed” and what does it say? Framing of any issue can have a large impact on its success. Much norm promotion is about persuasion, and the persuasiveness of appeal to adopt various norms will depend on how they are presented to potential adopters. Who are the promoters is part of the frame and its appeal (or lack thereof)? Great powers may not always be the most effective leaders for every effort. Victims (like Estonia) may have particular legitimacy and stature in promoting some norms. Where the proposed norm is located institutionally also matters to its future prospects. “Grafting” norms onto existing institutions has the advantage of avoiding bureaucratic start-up costs but it also ties the new norms to extant ones which may shape their future development in powerful ways. For example, many have argued that by choosing the Wassenaar Arrangement--a creature of Cold War security politics-- as the venue to develop norms (and laws) for internet based surveillance systems the emerging cybernorms favor security concerns over cyber responders and researchers’ needs. The alternative would be to push for a new institution or stand-alone process. The Freedom Online Coalition, the London Process, or the NetMundial initiative would be examples. This allows promoters to focus more squarely on distinctive needs in cyberspace but the effort then enjoys none of the resources or legitimacy 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 such that they can shut down discussion of new norms or keep them off the agenda. UNICEF enjoyed this kind of gatekeeper status and was able to stop efforts to build new norms around children born of war rape. More fundamentally, shared beliefs are dynamic; they change as contexts change, as new problems arise, and as group beliefs and group membership shift. A long-standing norm in warfare used be “to the victor goes the spoils.” Over the 20th century, acceptance of this norm waned among states who stopped recognizing territorial gains main by force of arms. Shared beliefs are rarely settled for all time but are in constant motion and recent events in Crimea suggest that even this long-settled norm may be in some flux.

That said, several features can contribute to a norm’s success. Influential and widely respected leadership in promotion of the norm can be important in building shared beliefs and getting 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 and succeeded in part precisely because they were not perceived as pursuing a geopolitical agenda. Connections constructed between a new norm and widely-accepted existing norms can similarly bolster attractiveness of the new norm’s claims and likelihood of adoption.