A HOOVER INSTITUTION ESSAY

China and the US Strategic Construction of Cybernorms: The Process Is the Product

DUNCAN B. HOLLIS

Aegis Paper Series No. 1704

How can states anticipate which behaviors other states will pursue or forgo? States employ various tools—deterrence, treaties, political commitments, customary rules, etc.—that attempt to do so. For all their diversity, such efforts share a common objective: to instantiate *norms*. In international relations, norms represent shared expectations about appropriate (or inappropriate) behavior within a given community.[1] Just as norms can set expectations for individual human behavior—what clothes we wear, what utensils we use, when we resort to violence—they provide powerful vehicles for structuring state behavior. Norms explain why states accept the propriety of territorial boundaries just as they explain the social condemnation that follows perceived violations.[2] And where states engage in behaviors that become unwanted, constructing new (or different) norms provides a pathway for reducing or eliminating them. Normative changes, for example, explain why "modern" states no longer engage in acts like slavery, plunder, or gunboat diplomacy.[3]

With such a legacy, it is not surprising that the United States turned to "cybernorms" to address the rising insecurity of cyberspace, especially where it could be attributed to key states like China.[4] For nearly a decade, the United States had two significant goals for affecting Chinese behavior in cyberspace: (1) dampening data theft from US commercial sources via cyber means; and (2) reducing the risk of an inadvertent armed conflict due to unaligned expectations of cyber "rules of the road."[5]

By its end, the Obama administration could point to achievements on both fronts.[6] In 2013, a United Nations Group of Governmental Experts (the UN GGE), including experts from both the US and Chinese governments, adopted a consensus report indicating that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communication technology] environment."[7] In September 2015, President Barack Obama and President Xi Jinping announced a "common

I am indebted to Spenser Karr for his research assistance. For helpful comments on this paper, I thank Martha Finnemore, Jack Goldsmith, and participants in the Hoover Institution's National Security, Technology, and Law Working Group at Stanford University. I also received financial support for this paper from the Hoover Institution and the US Government (via Minerva Grant No. N00014-13-1-0878). All errors or omissions, however, remain entirely my own.

understanding" on cyberespionage.[8] They agreed that neither the US nor the Chinese government "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing commercial advantages to companies or commercial sectors."[9]

Precisely how much to celebrate either deal has, however, proven a matter of some controversy. Some experts cited the 2013 GGE report as a landmark breakthrough, given earlier Chinese insistence on the need for new (rather than extant) international law when it comes to cyberspace.[10] On the other hand, critics question the sincerity of China's commitment given the GGE's subsequent inability to elaborate *how* international law would apply.[11] Similarly, praise for the Obama-Xi understanding ranged from a good step forward to a "historic" commitment.[12] Recent reports have noted a marked decline in commercial cyberespionage operations attributed to Chinese sources.[13] Some suggest, however, that this reduction simply reflects a move to more sophisticated, harder-to-observe methods.[14] Moreover, to the extent that there has been a shift in Chinese behavior, a 2016 FireEye report questioned whether it could be attributed to the Obama-Xi deal.[15] The report traced the decline to an earlier, internal decision by the Xi government to launch anticorruption reforms that led to more control over "illegitimate use of state resources."[16]

For the most part, these critics and proponents have measured both deals by focusing on their contents—on what they say. That approach certainly has merit. After all, both agreements derive from normative projects—efforts to create reliable expectations about China's future actions (or inactions). We cannot reliably assess their success (or failure) without attention to the phrasing and meaning of the agreements reached.

At the same time, such a content-only analysis is necessarily—and substantially—incomplete. Norms are not fiats, nor are they synonymous with agreement.[17] Rather, norms are inherently *social* constructs that emerge and spread by processes of interactions among particular groups of actors in specific contexts.[18] Thus, those who seek to establish a norm (so-called norm entrepreneurs) have many more choices beyond deciding what they want the norm to say, including (1) which other ingredients to employ in constructing a norm; (2) where they will do so; and (3) by what mechanisms they expect the norm to develop and evolve.[19]

For starters, norms—which social scientists describe as "collective expectations for the proper behavior of actors with a given identity"[20]—comprise not one, but four, distinct ingredients: (a) *behavior*—the action (or inaction) directed; (b) *identity*—the members of a specific community or group that accepts the norm; (c) *propriety*—the sources that justify delineating the proper or improper behavior (e.g., law, culture, religion, politics); and (d) *expectations*—the intersubjective understanding that gives the norm its social force among group members.[21] The quality of each of these ingredients can vary widely. Expected behavior, for example, can range in its depth from highly precise and certain "rules" to broad "principles" that outline general categories of action or inaction.[22] Norm

entrepreneurs must, therefore, decide which particular alignment of ingredients to pursue in crafting a norm.[23]

Second, norm entrepreneurs must decide *where* they will promote their norm.[24] They may do so by grafting it onto an existing institution or regime, thereby endeavoring to leverage the legitimacy and effectiveness that accompanied prior successful efforts.[25] Or, they may opt to promote a norm ad hoc, employing new processes tailor-made for the desired normative outcomes.[26]

Third, as with a recipe, the mechanisms by which norm ingredients are combined matter. Norm entrepreneurs have different tools that they may deploy—whether alone or in combination—to form or spread their desired norm. These mechanisms divide (loosely) into three categories: (1) incentives (positive "bribes" and negative "sanctions"); (2) persuasive arguments; and (3) socialization measures (e.g., naming and shaming, professional training).[27]

Thus, norm entrepreneurs like the United States must attend to many more choices than what they want a norm to say (as important as that choice might be). Such choices are, moreover, often consequential—each involves potential risks and rewards that can shape a norm's realization and effectiveness. As such, the unit of analysis for a norm lies not in its mere visible manifestation in some agreement, but in the strategic construction of the processes in which that agreement is situated. Simply put, the process *is* the product of any normative project.[28]

The strategic consequences of a process-oriented analysis of cybernorms are evident in the choices that underpin both the 2013 UN GGE consensus on the application of international law (what I call the "IL norm") and the Obama-Xi understanding on state-sponsored commercial cyberespionage (the "CCE norm"). Along all the metrics listed above—ingredients, location, and mechanisms—the two projects reflect very different choices. Such comparisons do not reveal all the choices open to norm entrepreneurs nor are they (yet) sufficiently robust to endorse specific choices for particular contexts.[29] But they do illustrate the wide spectrum along which such choices may be made. More important, they offer a new lens for assessing ways in which the evolution of norms and their interaction are empowered or constrained by chosen ingredients and mechanisms. States (and scholars) would thus do well to assess current and future efforts to construct cybernorms with China by looking at not just one, but all aspects of the normative process.

Beyond the trade-offs it reveals in designing cybernorms, a process-oriented vision also provides the necessary foundation for situating these projects within broader contexts. Cyberspace is rife with various norms in manifold communities across a range of topics. Domestic and international laws, political processes, and technical protocols already reflect significant normative commitments at different stages of development and diffusion.[30] Thus, decisions about whether to pursue a specific normative ingredient (or a particular location or a certain mechanism) must attend not just to the range of alternatives but to how each

choice will map onto existing normative frameworks. Success is far from assured. Indeed, even as it seeks to change Chinese behavior via the IL and CCE norms, it is important to recognize that the United States does not hold a monopoly on norm entrepreneurship. China can—and does—have a normative agenda of its own (most notably in its pursuit of norms tied to the concept of "cyber sovereignty").[31] Any strategic construction of US cybernorms must anticipate how China's own norm promotion efforts may affect US efforts, whether by successfully shifting expectations among other states or by altering the United States' own expectations of what constitutes appropriate behavior in cyberspace.[32]

Norm Promotion: Which Ingredients?

For the United States, pursuing the IL norm involved a very different set of choices than for its pursuit of the CCE norm. The two norms involve very different categories of behavior, different group identities, different sources of propriety, and different intersubjective understandings. Such differences, moreover, led to different opportunities (and constraints) for the resulting norm processes themselves.

Behavior—Rules or Principles?

Cybernorms can direct behavior at various levels of precision, most notably via rules, standards, and principles.[33] Rules are precise enough to allow an ex-ante appreciation of what the behavior involves. Standards, in contrast, involve directions (i.e., "reasonable" behavior) that are best evaluated ex-post in light of all the facts or some background policy. Principles, meanwhile, set forth only general courses of conduct under which many behavioral options remain open.[34]

Looking at our two examples, the CCE norm is clearly embodied in a rule while the IL norm states a principle. As a rule, the CCE norm is framed with precision. It identifies the norm's subjects (the US and Chinese governments) and clarifies specific actions to avoid (conducting or knowingly supporting) with respect to a defined object ("cyber-enabled theft of intellectual property, including trade secrets or other confidential business information") and a defined purpose (for "competitive advantages").[35] By tailoring the norm with such detail on "who should do what," the CCE norm provides a level of certainty about its expectations and ready boundaries for its application.[36] Of course, there will always be interpretative ambiguities (i.e., what does it mean to "knowingly support" cyberespionage?) just as there will be questions of fact (i.e., whether an intellectual property cyber theft was done with the "intent of providing competitive advantages"?).[37] As a rule, however, the CCE norm cabins such questions to a discrete checklist against which the norm's subjects (and third parties) may measure conformance. Thus, whether or not the CCE norm is the proximate cause, the reduction in cyberespionage against commercial targets conforms to it.

At the same time, however, rules carry a rigidity that may create difficulties for norm processes.[38] Rules assume the norm subject's capacity to conform.[39] In the CCE context, this creates

questions about *why* there is continued reporting of commercial cyberespionage—is it due to the Chinese government's unwillingness to comply or, despite Xi's recent efforts, will some Chinese agents retain autonomy to slip the bonds of central control?[40] Moreover, where circumstances are subject to rapid change—as is the case in the ICT environment—rules may lack the flexibility to adjust.[41] For example, the CCE rule only speaks of intellectual property theft for commercial advantage, leaving it unavailable if new malware practices (e.g., ransomware) are repurposed for a commercial advantage (i.e., targeting competitor systems and networks).

Principles, in contrast, have more imprecise formulations that trade behavioral certainty for flexibility.[42] They contemplate behavioral expectation but with such breadth that the norm's subjects may treat a wide swath of behavior as conformance. The IL norm, for example, is framed in a passive voice, identifying the norm's subjects—states—only by implication, and then only directing them to treat a broad concept—international law—as applicable. This leaves China (or the United States for that matter) ample room to assert conformance since—unlike the CCE norm—the principle's terms lack the means for verifying conformance with its contents. Of course, in the right circumstances, this may be more a feature of principles than a bug. The IL norm gains its force by operating as an umbrella, covering a broad range of norms associated with international law, thereby allowing it to become a proxy for a range of normative claims instead of just one. Thus, China's accession to the IL norm implicates questions about its conformance with a whole range of more specific international law rules and standards (e.g., the law of armed conflict, human rights, state responsibility). Indeed, one might view China's ongoing push for "cyber sovereignty" as an effort to narrow how international law applies or otherwise expand the range of its own domestic jurisdiction.[43] As such, the IL norm—and the competing interpretations ascribed to it by the United States and China—may end up having broader systemic implications for the Sino-US relationship (let alone cyberspace itself) than the narrower range of conduct engaged by the CCE norm.[44] Moreover, the IL principle has flexibility; if international law changes (i.e., states negotiate a new global treaty), the norm can accommodate such developments.

None of this is to suggest that the IL principle was a better choice than the CCE rule (or vice versa). Their effectiveness must be measured, not against each other, but with respect to the goal that motivated the United States to promote them in the first place. The success of the CCE norm may turn on concrete analyses of Chinese behavior, but it would be a mistake to measure the IL norm along similar lines. In its initial iteration, the IL norm sought to avoid unwanted future behavior by China (e.g., threats to international peace and security, armed conflict) more than it targeted ongoing behavior. Thus, it is much harder to analyze the efficacy of the IL norm where the lack of activity (i.e., the unwanted behavior) may be attributable to the norm, or may be accounted for by a range of other possible explanations, creating a measurement problem of sorts. Such different functions make comparisons of the norms' relative efficacy difficult. Still, there are clear trade-offs involved in the choice to pursue a rule or a principle (or, for that matter, a standard) that demonstrably affect the contours of both the IL and CCE norms.

Identity—Which Group Should a Norm Target?

Norms make behavioral claims on a group (or community) of actors based on their identity with that group.[45] For example, individuals who are identified as physicians have certain norms, just as do entities that claim the status of nation-states. Of course, both individuals and states will belong to more than one group at the same time. In the ICT context, for example, China's communities include all nation-states, like-minded ones (e.g., the Shanghai Cooperation Organization), bilateral relationships, and multistakeholder groupings (e.g., ICANN, the Internet Corporation for Assigned Names and Numbers). Moreover, actors within China may also comprise a discrete group (e.g., members of its ICT industry) that may be subject to a separate suite of normative claims.

China's various communal ties present a range of identities that the United States may tap into to pursue norms. And in the IL and CCE cases, the United States tapped very different group identities. The IL norm was targeted at all states, including China. In contrast, the CCE norm originated with a community of two—the United States and China. As with the selection of rules, principles, and standards, the selected group affects the shape of the norm processes that emerge.

By opting for a bilateral formulation, the United States was able to tailor the CCE norm's contents to the problem it wanted solved.[46] Although gaining China's acceptance was reportedly not easy, the bilateral formula avoided the transaction costs of including additional parties.[47] It is an approach particularly appropriate for the powerful—where there is no need to incorporate the power or expertise of additional actors because their capacity or consensus is unnecessary. Indeed, by going bilateral the United States may have actually signaled a greater respect for China's power and capacity in cyber operations than if it had pursued a larger plurilateral or global norm at the outset (an acknowledgement that might, in turn, help explain China's eventual acquiescence). Of course, US efforts may still produce success on those broader identity fronts since, as the reaction to the creation of the CCE norm shows, mimicry is possible. Other powerful states (e.g., the United Kingdom, Germany) sought to secure China's accession to a similar norm bilaterally, leading eventually to the CCE norm's adoption in the G-20's pluri-lateral forum of the most powerful nations.[48]

On the other hand, by going bilateral, the United States sent a signal that it had specialized interests in China's behavior that suggested it had less concern with similar actions by other actors. Thus, by going bilateral, the United States had to forgo potentially broader gains from a norm that could have included other states which might engage in similar behavior, such as Iran, Israel, or Russia.[49] Even vis-à-vis China, the force of the CCE norm may remain unclear, given the risk that China could find another normative claim on its identity (e.g., derived from its cybersecurity treaty with Russia) to be more important when the two compete or conflict.[50] Indeed, it is even possible that China's own understanding of the

norm concept might be sufficiently different from that of the United States such that more direct bilateral confrontations over its application could occur.[51]

In contrast, the IL norm is structured as a global norm for all states. China is treated as one of the nearly two hundred nation-states potentially subject to this rule. The upside of going global lies in its systemic potential—global norms for all states may stabilize behavior generally by reducing normative competition and conflicts that can pull at a state like China when they are set in bilateral and plurilateral contexts. On the other hand, a norm for all states necessarily involves a much wider array of interests and values, leading (generally) to shallower contents.[52] Indeed, the IL norm may be a paradigmatic case of a lowest common denominator norm. It is possible that, over time, global norms can build confidence leading to deeper normative commitments.[53] But such temporal issues may trade off against the potential for more immediate results among a smaller grouping.

Of course, in pursuing deals with China, both the IL and CCE norms assume China has the capacity to conform. That may not be much of an issue with respect to the IL norm given the centrality of states to the international legal order. But the CCE norm's focus on the Chinese government does at least raise the possibility of a coverage gap for China-based commercial cyberespionage that the Chinese government does not "conduct or knowingly support."[54] To accommodate cases where the relevant behavior involves state *and* non-state actors, the United States could have considered constructing the norm around different group identities, such as a multistakeholder grouping or even the global ICT industry if it were determined to have the most capacity to make the desired norm effective.

Propriety—The Source of a Norm's Claim for Conformity

The United States has an array of different sources for separating proper from improper behavior in cyberspace, including law, political commitments, professional training, and culture.[55] For its part, China has chosen to push a conventional source (i.e., a new global treaty) for its own norm promotion efforts, with the United States being the one to resist the idea of situating cybernorms in an international legal instrument.[56] In doing so, the United States has resisted the credibility that a treaty might provide, presumably out of concerns over difficulties in reaching agreement internationally, the increasingly stalled US domestic approval process, or the "lock-in" effects that treaties generate.[57]

Whatever its concerns about a treaty, the IL norm shows that the United States does not object to using international law as the basis for a norm's propriety. Indeed, the invocation of the social forces of international law appears to be the whole point of the IL norm.[58] But such an invocation comes with conditions, positive and negative. On the one hand, relying on international law brings in an attendant set of norms for responding to nonconforming behavior (e.g., the law of state responsibility).[59] There is no need for the normative process to construct additional compliance mechanisms because such mechanisms exist by default.

On the other hand, the exact reasons why international law matters remain disputed. Some suggest there is a socialization of international law that exerts a substantial compliance pull on state behavior, while for others, most international law norm conformance tracks national interests.[60] As such, critics sometimes wonder about what exactly is gained by invoking the mantle of international law.[61]

In contrast, the CCE norm does not come with the baggage of existing international legal processes or ontological questions. Rather, it was carefully (but quickly) framed in nonlegal terms. It draws its authority from the political force of the "common understanding" among Presidents Obama and Xi. The speed at which appropriate lines can be drawn is a key benefit for norms that rest on the force of politics (in contrast to the often drawn-out procedural processes associated with legal norms, whether domestic or international).[62] Similarly, to the extent the CCE norm sources to a political process, that process can change rapidly. If, for example, the Trump administration decides the political calculus has shifted, the CCE norm might be destabilized. Conversely, China might decide that the political commitment to one president (Obama) is not suited to another (Trump). And that is one of the downsides of using politics as a source of propriety; the more malleable nature of politics means its norms likely lack the credibility and stability that accompany law or the deeper seeded expectations of a particular culture.

It is possible, of course, for norms to derive their propriety from multiple sources. Thus, the IL norm emerged as the product of an (often heated) political negotiation, making it rest on politics as well as international law. And for the CCE norm, US domestic law provided another source of authority—alleged Chinese violations of which led to the indictments of five People's Liberation Army (PLA) officers more than a year before the Obama-Xi deal.[63] Naturally, China may resist tying a norm's propriety to the requirements of foreign law. Yet China's recent cybersecurity law suggests it also recognizes the value of domestic legal authority as part of broader norm promotion efforts.[64] In either case, it is clear that the CCE norm's alignment with US domestic law enabled sanctions that may have played a role in getting China to consent to the CCE norm directly.[65] This suggests that norm promotion efforts may be done sequentially.[66] In other words, the United States may choose to invoke a particular source for a norm's propriety at Time 1 (e.g., domestic law) only to shift to a different source at Time 2 as the norm's subjects show a willingness to internalize and act on it (i.e., via a political commitment). Of course, depending on the circumstances the sequence might be reversed, beginning with cultural expectations or a political commitment that is later instantiated in law. There is no fixed recipe for balancing trade-offs or sequencing different sources of propriety, but greater awareness of the options makes for better strategies.[67]

Expectations—What Type of Internalization to Seek?

For sociology, the norm's gold standard for shared expectations is full internalization—where the expectations are so ingrained among members of a community that they perform them without thinking.[68] Full internalization has its attraction to those seeking

cybernorms. Since the attribution problem complicates the ability of group members to observe the propriety of each other's behavior, a norm that is performed without the need for monitoring or verification would be attractive.[69] Yet, full internalization also has its downsides. Settling expectations may not be socially optimal in a rapidly changing ICT environment; it risks creating path dependencies at the expense of normative shifts that might improve the stability and security of cyberspace overall.

On the other end of the spectrum are norms that receive mere lip service, where members of the group acknowledge the norm but some act inconsistently with its expectations.[70] The insincerity of these expectations may cause obvious problems for the norm to achieve its desired goal. And yet insincerely shared expectations may be better than no expectations at all. Over time, social forces (i.e., cognitive dissonance, organizational platforms) can transmute insincerity into more deeply shared expectations of proper behavior.[71] The Helsinki Accords serve as the paradigmatic example where initial Soviet insincerity on human rights eventually transformed into acceptance of a global system of human rights monitoring and organizations.[72]

Originally, many suspected the CCE norm fell into the lip service category, although reports by FireEye and others suggest that China has actually altered its behavior in significant ways.[73] In fact, the IL norm may be a better example of lip service. To date, China has said that it accepts international law's application to cyberspace but continues to resist moves to elaborate how specific fields of international law—most notably the laws of armed conflict—do so. Whether continued calls for China to explain its understanding of the extant law in various forums like the GGE will shift its expectations remains to be seen. In any case, as the Helsinki example suggests, we should not be too quick to read the IL norm's expectations as entirely ineffectual.

More important, norm entrepreneurs constructing a cybernorm may target a much broader spectrum of shared expectations than just the poles of full internalization and insincerity. For example, some normative expectations may become, in the words of Cass Sunstein, incompletely theorized: states recognize and perform the delineated behavior as proper without agreeing on why they do so.[74] For example, to the extent China does conform to the IL norm, it may do so because it wants to invoke international law principles like sovereignty, which in turn help empower control over content and traffic on its own networks.[75] The United States, in contrast, likely wants international law to apply because it can act as a restraint on aggressive behavior by China and others against the United States, private industry, or individual civil liberties. The latest information also suggests that the CCE norm may be incompletely theorized as China conforms for internal reasons different from the security risks that motivated the United States' initial promotion efforts.[76]

Incompletely theorized agreements offer a glass that can be seen as half full or half empty. On the one hand, these shared expectations involve concrete behaviors that conform to the norm's contents. As such, they may be more effective than insincere accommodations to norm promotion efforts. On the other hand, these expectations are not fully internalized

Table 1. The Ingredients of US-China Cybernorms

Normative Ingredients	*Choices*		
	2013 UN GGE Report on the application of international law	**Obama-Xi Statement on cyberespionage for commercial advantage**	**Other options**
Behavior	Principle	Rule	Standard
Identity	Universal (all States)	Bilateral (US-China)	Plurilateral, Multistakeholder, Private Ordering
Propriety	International Law, Politics	Politics, Domestic Law	Culture, Professional Standards
Expectations	Lip Service	Incompletely Theorized	Fully Internalized

because of some (often significant) differences in values or interests. This means that, as the norm iterates over time, tensions are likely to emerge where these values or interests may push group members in different directions when it comes to performing the norm or seeking to alter its contents. For example, if national security interests are driving Chinese expectations on the CCE norm, one could imagine China interpreting the category of cyberespionage for commercial advantage to exclude espionage against commercial entities in places like Japan or Taiwan on the grounds that it implicates national security even if it also produces economic losses for those actors targeted.[77]

Taken together, we see that the IL and CCE norms involved different types of ingredients. The United States had to decide how precisely it wanted to define the desired behavior, for which group it would do so, on what basis of propriety, and with what targeted end-stage of expectations. Moreover, as discussed above, these choices have strategic significance, involving possibilities and perils that can influence the resulting norm process. Table 1 summarizes the selections made for both IL and CCE norms as well as those options left on the table.

Location: Whether to Graft Norms or Institute Ad Hoc Processes

Having decided the structural framework for a norm, entrepreneurs must still decide where they want to situate its processes. International relations scholars have noted, for example, the potential benefits of grafting—integrating a norm process within an existing institution or regime.[78] Grafting heightens the visibility of the norm process and, to the extent the host institution has legitimacy and a track record, lends that aura to it as well. Where the norm is constructed and processed in a well-known forum, its subjects may be more likely to accept it and perhaps even internalize it more quickly.[79]

The IL norm clearly follows the grafting path. The United States pushed it in one of the more visible of international institutional platforms: the UN General Assembly's First

Committee.[80] Moreover, it sought to advance the norm through a process—a GGE—that had precedents and successes in other areas where novel developments required collective responses.[81] As such, when the GGE concluded in 2013 (and again in 2015) that international law applied, the world took notice of the consensus (especially China's role therein).[82]

Yet grafting has its limits. The organizational processes and cultures of the host institution cabin the norm's development. It is no coincidence that when states and scholars discuss the IL norm's meaning they almost always refer to those aspects of international law concerned with international peace and security (e.g., the prohibition on the use of force and the law of armed conflict). That scope tracks the disarmament and arms control mission of the First Committee.[83] As such, the grafted IL norm is self-limiting. Despite the critical importance of international law's application to a broader array of ICT issues—like human rights or transnational cybercrime—these aspects of the IL norm have received relatively little attention. Indeed, to the extent such issues are raised in the GGE process, they are dismissed as outside the ambit of the process itself.

Similarly, to the extent one sees a greater role for the ICT industry in the maintenance of international peace and security than in other contexts, it might make sense to pursue norms in settings where those actors could have a voice. By choosing the GGE, however, this option is foreclosed; the GGE is a closed, non-transparent process made up solely of states. As such we might predict its norms, including those on international law, will feature different contents or points of emphasis than if the norms were located in a more multi-stakeholder setting.

Instead of grafting, cybernorm entrepreneurs can also stand up ad hoc norm processes. Ad hoc processes may be tailored to the problem presented without the constraints of a preexisting organization's membership, mission, or values. The CCE norm started out as such a case. In fact, it was notably absent from the list of US norms promoted at the GGE.[84] Instead, Presidents Obama and Xi reached a common understanding that addressed their mutual concerns. The fact that they represent two of the world's largest powers meant that they did not need the visibility that grafting offers.

On the other hand, the theatrics surrounding the Obama-Xi joint statement were substantial. It required a significant investment of personnel and resources, with regularly scheduled meetings among various ministers and principals, alongside logistical challenges like setting up communication mechanisms that most standing organizations worked through long ago.[85] And unlike the stability afforded by preexisting institutions, the durability of the CCE norm's follow-on processes is much less assured. Those who pushed the original understanding (the Obama administration) have been replaced by new actors (the Trump administration).[86] Moreover, the CCE norm process remains one among many in an age of "infinite meetings."[87] Its importance and priority to China vis-à-vis other processes (e.g., the World Internet Conference, the Shanghai Cooperation Organization) remain unclear.[88]

Mechanisms: Choosing the Tools for Norm Promotion

Once a norm has been framed in terms of its ingredients and located in an existing or new process, there remains the choice of tools—incentives, persuasion, and/or socialization—to promote and distribute it.[89] Properly aligned incentives have demonstrated a capacity to control behavior, which may explain why the United States chose incentives in its quest for the CCE norm. Its incentives came in both positive and negative forms. The United States undertook a series of documented steps designed to penalize China for its unwanted behavior, including indicting members of the PLA, drafting a sanctions regime, and threatening to deploy it.[90] At the same time, some reporting suggests that China undertook the CCE norm in return for a positive incentive—a US decision not to respond to China's hacking of the Office of Personnel Management, which as traditional espionage otherwise fell outside the CCE norm's ambit.[91]

The use of incentives may work to control Chinese behavior for a time, but they also can pose a problem of continuity. For incentives to work, the United States must maintain the will and resources to keep up incentives indefinitely or long enough for socialization processes to take hold. If China perceives that the United States' political will to divide commercial cyberespionage from more traditional variants is fading, it opens up the possibility of a Chinese backlash where the government authorizes renewed commercial cyberespionage activities (a scenario that may be worse than the situation before the norm promotion efforts began, if one assumes that some of the pre-2015 commercial cyberespionage was done by unauthorized government agents or actors).[92]

Of course, the United States did not limit itself to incentivizing the CCE norm. It also used public and diplomatic communication channels to try to persuade China of the propriety of making the distinction between espionage for commercial and security purposes.[93] Persuasion has obvious appeal for norm entrepreneurs since the persuaded are more likely to fully internalize the norm.[94] The question becomes how to tell when persuasion has taken hold. For example, are ongoing reductions in commercial cyberespionage by China a reasoned acceptance of US arguments? Or are they motivated by other factors (e.g., the desire for more centralized control or a desire to avoid public exposure of Chinese operations)?[95] When motivations for nonconforming behavior are hard to observe, persuasion is difficult to assess. Moreover, it is no secret that Chinese and US officials operate pursuant to different value systems, and such differences complicate persuasive mechanisms. Where the values are unaligned, the best the US normative outcome may achieve is the aforementioned incompletely theorized norm where China and the United States accept the same behavioral conditions, albeit for very different reasons.[96]

Unlike the CCE norm, persuasion appears to have been the central tool for advancing the IL norm, with the United States using the GGE meetings as a key forum for persuading China (and other states) of the value in recognizing the applicability of international law.

In larger groups such as this, however, the United States faces the risk of "norm capture."[97] The United States may have successfully persuaded the GGE on the existence of the IL norm with the expectation that doing so would trigger deeper conversations about the use of force or the law of armed conflict. But China, along with some other GGE members, has sought to repurpose the norm to align with its own interests in advocating other areas of international law, namely, sovereignty.[98] As such, China and other states may have been persuaded to apply international law to support a very different set of activities than those envisioned by the United States.

Beyond incentives and persuasion, tools of social influence, such as naming and shaming or capacity-building, may also be deployed to promote and distribute norms.[99] By publicizing what is seen as nonconforming behavior, naming and shaming reinforces the norm's existence and invokes the social pressures of group membership on any nonconforming actor.[100] Naming and shaming featured prominently in the US promotion of the CCE norm, including its endorsement of the Mandiant Company's report (on Chinese cyberespionage), anonymous US official quotes in the media, and, of course, the indictment of individual PLA officers for their activities.[101] Indeed, given the unlikelihood that those officers would ever come within US jurisdiction, the entire purpose of the PLA indictments was apparently to name and shame China into a change of behavior.

Naming-and-shaming efforts work best where the violator has the capacity to conform and has a strong affiliation with the community within which the norm exists.[102] Where the community is not "tight," there's a risk that the violator may decide membership is not worth the costs of conformity.[103] Such a risk is very real for a group made up of the United States and China. That pairing is not tight, unlike, for example, the US relationship with the United Kingdom. By expanding that group over time to include the whole G-20, however, there may be greater social pressures to conform as that is an identity that China may be more reluctant to sever.

Socialization may also come through capacity-building for the norm itself, whether in the form of technical assistance, training, or the establishment of communication networks.[104] Thus, the United States and China have pursued the construction of a hotline.[105] That hotline will provide an opportunity for repeated interactions among US and Chinese officials to pursue the CCE and other norms (including those promoted by China). This may create a more communal basis for their interactions, which may, over time, strengthen the force of the norms themselves. For the IL norm, by contrast, capacity-building has come through training workshops. In 2016, for example, the GGE hosted a workshop including GGE members alongside international lawyers and other experts to discuss the application of international law in cyberspace. Exercises like this create opportunities for group members to learn about appropriate expectations and to adjust their behavior accordingly. How effective they are in shifting China's behavior specifically may be open to question. China has its own community of international lawyers who often approach the law quite differently from their US counterparts, as past Track 2 efforts have shown.[106]

Table 2. Mechanisms for Promoting Cybernorms with China

Norm Project	*Mechanism*				
	Incentives			**Socialization**	
	Positive	**Negative**	**Persuasion**	**Naming & Shaming**	**Capacity-Building**
IL Norm			✓		✓
CCE Norm	✓	✓	✓	✓	✓

Stepping back, as summarized in table 2, the United States employed a limited set of mechanisms to pursue the IL norm. In contrast, it used almost every available tool to gain China's acceptance of the CCE norm, which shows that these mechanisms are not mutually exclusive. Indeed, the CCE kitchen-sink approach has its advantages, whether on the theory that deploying multiple processes increases the chances that one will gain traction with China or that their combination may operate as a force multiplier. On the other hand, the United States may not always want to combine mechanisms. In other contexts, incentives have been shown to undermine socialization, leading group members to regard conformance in economic (i.e., "what are the costs and benefits of my non-conformance") rather than social terms (i.e., "if I want to be a responsible state I should do X and not do Y").[107] It is even possible that employing strategies in one process can have crossover effects on other norm projects. For example, as Adam Segal has noted, the US naming-and-shaming strategy with respect to the CCE norm has been tied to Chinese and Russian insistence on an evidentiary threshold for alleging violations of the IL norm (specifically, that allegations of internationally wrongful cyber behavior by a state "should be substantiated").[108]

Conclusion

How should we evaluate the success of US foreign policy on China and cybersecurity? It is certainly tempting to focus on the texts of negotiated products like the Obama-Xi common understanding or reports from the likes of the GGE in which the United States and China participated. To do so, however, misunderstands the very nature of these agreements. These are normative projects that aspire to achieve US interests in affecting Chinese behavior by getting China to share certain expectations of proper (or improper) behavior based on its identity with one or more communities of actors. As such, they involve more ingredients than just an agreement on some specified behavior; they implicate issues of identity, propriety, and expectations as well. At the same time, it matters where the United States promotes the norm and the particular cocktail of mechanisms it employs to do so.

For each element of the norm and the process by which it is formed and spread, the United States had choices to make. Whether or not it made those choices conscientiously, each had strategic significance. Pursuing a rule for the CCE norm provided opportunities for measurement that are absent for principles like the IL norm. Pushing the CCE norm

bilaterally may have shown China sufficient respect to engender its acquiescence, but it excluded other states whose commercial cyberespionage activities may be problematic now or in the future. Understanding the particular implications of these choices not only helps us better understand the IL and CCE norms but also provides a menu that US policy makers may wish to consider in pursuing future cybernorms with China.[109]

As important as the choices on the norm's architecture are, the questions about the processes for constructing it are of equal significance. Using the UN GGE to promote the IL norm allowed the United States to graft onto that framework's legitimacy and past success even as its mission cabined the reach of any normative outputs to the security context. Similarly, it matters that the United States opted for a more ad hoc process for the CCE norm when it could have chosen to group that norm within the suite of those it was promoting at the United Nations. And, of course, the tools deployed to do this promoting implicate the effectiveness of the project in various ways; incentives may bring actors into conformance more quickly but require a continued investment of resources. In contrast, socialization takes more time, but offers the promise of fuller internalization. In other words, the mechanisms chosen can significantly affect the substantive content of the normative product that results.[110] Taken together, it becomes clear that the success (or failure) of US normative efforts depends on their processes.

On a more fundamental level, we might even say that the norm process is the desired product. That process—rather than any specific agreement or "deliverable"—should be the unit of analysis to evaluate the effectiveness of US norm promotion efforts. True, measuring the success or effectiveness of a process is substantially more difficult than measuring compliance with a written commitment. But it is also likely to be a more accurate gauge for explaining and predicting state behavior.

Each time the United States or China acts under the banner of the IL or CCE norms, each has to decide what these norms mean and what behavior(s) they require. Each of these interpretations creates episodes of conformity (or nonconformity) that accrete and shape the expectations of the norm's meaning.[111] Thus, to understand how these norms affect state behavior we have to pay just as much attention to how state behavior affects the contents and contours of the norms themselves. In other words, norms are inherently dynamic processes that emerge and spread (or even die) over time. A process-centered theory of norms accommodates this dynamism in ways more traditional analyses of compliance do not.

Of course, the United States should expect unforeseen circumstances and the (natural) evolution of norms themselves. And as these changes occur, the strategic calculus may need to change, making norm construction not a set of onetime decisions, but an ongoing process of decision making. For present purposes, this means that the United States cannot let up in its push for international law or a prohibition on commercial cyberespionage. It also needs to pay attention to Chinese norm promotion efforts and to evaluate whether and

how they may affect those behavioral expectations that the United States wants to maintain or instantiate as proper in cyberspace.

As noted at the outset, efforts to promote norms do not occur in isolation. Norms emerge from existing contexts and against the backdrop of other norms and other norm entrepreneurs. The cybersecurity landscape is a pluralistic environment where the successful pull of conformity of one norm on an actor like China can reinforce *or undermine* its conformity with others. For example, although it has been careful to deny any legal force to the CCE norm, the United States must be aware that instantiating such a norm may affect the IL norm, a field that has long had an uneasy relationship with espionage.[112] Accepting a norm prohibiting at least some forms of cyberespionage may reverberate with those favoring international legal regulation of espionage to the detriment of those who believe intelligence collection should lie beyond the international lawyer's reach.[113]

In the end, US policy makers have a hard job to do in evaluating existing and future normative projects with China. They must focus on an array of ingredients, locations, and processes, sensitive to the role of time, existing norms, and competing norm promotion efforts by China (and others). In doing so, America may not always be able to answer which choices will lead to more effective norms. Indeed, it is not yet clear that the cyberespionage deal was more successful than the agreement on international law (or vice versa). But, the United States can clearly benefit from strategic thinking about how norm processes with China will succeed or fail as much in the processes by which they operate as any particular deliverables they achieve.

NOTES

1 See Peter J. Katzenstein, "Introduction: Alternative Perspectives on National Security," in *The Culture of National Security: Norms and Identity in World Politics,* edited by Peter J. Katzenstein (New York: Columbia University Press, 1996) 1, 5; Martha Finnemore, *National Interests in International Society* (Ithaca, NY: Cornell University Press, 1996), 22–23. Of course, in other disciplines, like mathematics, the term "norm" carries an entirely different meaning.

2 See, e.g., UN General Assembly Res. 68/262, UN Doc. A/Res/68/262, March 27, 2014 (affirming the territorial integrity of Ukraine and underscoring the invalidity of the 2014 Crimean referendum). Of course, norms may be contested, in terms of either their meaning (e.g., Russia's competing interpretations of territoriality norms with respect to Crimea) or their very existence (e.g., debates over a norm permitting humanitarian intervention).

3 See, e.g., Wayne Sandholtz, *Prohibiting Plunder: How Norms Change* (New York: Oxford University Press, 2007); Martha Finnemore, *The Purpose of Intervention: Changing Beliefs about the Use of Force* (Ithaca, NY: Cornell University Press, 2003), chap. 2.

4 See Martha Finnemore and Duncan Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (July 2016): 425, 436–37.

5 See, e.g., Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," May 7, 2013, 36, http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf; US Department of State, "Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues," news release, June 7, 2013, https://2009-2017.state.gov/r/pa/prs/ps/2013/06/210418.htm;

"Admit Nothing and Deny Everything: Barack Obama Says He Is Ready to Talk with Xi Jinping about Chinese Cyber-Attacks. That Makes One of Them," *The Economist,* June 8, 2013, www.economist.com/news/china/21579044-barack-obama-says-he-ready-talk-xi-jinping-about-chinese-cyber-attacks-makes-one; Roger Hurwitz, ed., "A Call to Cyber Norms: Discussions at the Harvard-MIT–University of Toronto Cyber Norms Workshops, 2011 and 2012," 2015, 9.

6 I do not mean to suggest that these were the only such achievements. In 2015, the United States celebrated the UN GGE consensus report's adoption of several "voluntary" (i.e., nonlegally binding) norms of responsible state behavior in cyberspace, including prohibitions on targeting critical infrastructure and the work of computer security incident response teams (CSIRTs). See "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Office for Disarmament Affairs, ¶13(h), (k), UN Doc. A/70/174, July 22, 2015; State Department, "Statement on Consensus." Although significant achievements, I do not examine them closely here since the two examples I do analyze—international law and commercial cyberespionage—offer a sufficiently broad spectrum of strategic options for cybernorm construction.

7 See "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013, ¶19, UN Doc. A/68/98.

8 Demetri Sevastopulo and Geoff Dyer, "Obama and Xi in Deal on Cyber Espionage," *Financial Times,* September 25, 2015, https://www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644?mhq5j=e1.

9 See Office of White House Press Secretary, "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

10 See Joseph Marks, "U.N. Body Agrees to U.S. Norms in Cyberspace," *Politico,* July 9, 2015, www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900; Adam Segal, "The UN's Group of Governmental Experts on Cybersecurity," *Net Politics* (blog,) Council on Foreign Relations, April 13, 2015, https://www.cfr.org/blog-post/uns-group-governmental-experts-cybersecurity; see also Matthew Waxman, "Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Law Studies* 89 (2013): 109, 115 (noting Chinese calls for new international legal regulation).

11 See, e.g., Elaine Korzak, "International Law and the UN GGE Report on Information Security," *Just Security,* December 2, 2015, https://www.justsecurity.org/28062/international-law-gge-report-information-security; David Fidler, "The UN GGE on Cybersecurity: How International Law Applies to Cyberspace," *Net Politics* (blog), Council on Foreign Relations, April 14, 2015, https://www.cfr.org/blog/un-gge-cybersecurity-how-international-law-applies-cyberspace; Kristen Eichensehr, "International Cyber Governance: Engagement without Agreement?" *Just Security,* February 2, 2015, https://www.justsecurity.org/19599/international-cyber-governance-engagement-agreement. The 2015 GGE (largely) reiterated the 2013 consensus on international law's application, listed a few specific areas of international law, and called for further study. See 2015 GGE Report, ¶¶24–29.

12 Qian Ruisha, "U.S. Experts Hail China-U.S. Consensus on Cyber Security as 'Significant,'" *Xinhua,* September 27, 2015, http://china.org.cn/xivisitus2015/2015-09/27/content_36693188.htm; Paul Wiseman and Ken Dilanian, "Analysis: US-China Agreement on Commercial Cybertheft a Breakthrough—and a First Step," *U.S. News & World Report,* September 26, 2015, https://www.usnews.com/news/business/articles/2015/09/26/analysis-us-china-agreement-on-cybertheft-a-first-step; Kim Zetter, "US and China Reach Historic Agreement on Economic Espionage," *Wired,* September 25, 2015, https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage.

13 See, e.g., Patrick Howell O'Neill, "DNI: Chinese Hacking Against U.S. Companies is 'Ongoing' but 'Significantly Reduced,'" *Cyberscoop,* May 23, 2017, https://www.cyberscoop.com/china-us-hacking-odni-dan-coats-2017; Emilio Iasiello, "Ramping Down Chinese Commercial Cyber Espionage," *Foreign Policy Journal,* December 9, 2015, https://www.foreignpolicyjournal.com/2015/12/09/ramping-down-chinese-cyber-espionage.

14 See, e.g., Joseph Steinberg, "10 Issues with the China-US Cybersecurity Agreement," *Inc.,* September 27, 2015, https://www.inc.com/joseph-steinberg/why-the-china-us-cybersecurity-agreement-will-fail.html; Josh Chin,

"Inside the Slow Workings of the U.S.-China Cybersecurity Agreement," *Wall Street Journal,* June 15, 2016, https://blogs.wsj.com/chinarealtime/2016/06/15/inside-the-slow-workings-of-the-u-s-china-cybersecurity-agreement.

15 "Red Line Drawn: China Recalculates its Use of Cyber Espionage," FireEye, June 2016, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

16 Ibid. See also Jack Goldsmith, "U.S. Attribution of China's Cyber-Theft Aids Xi's Centralization and Anti-Corruption Efforts," *Lawfare* (blog), June 21, 2016, https://www.lawfareblog.com/us-attribution-chinas-cyber-theft-aids-xis-centralization-and-anti-corruption-efforts.

17 See Finnemore and Hollis, "Constructing Norms for Global Cybersecurity," 427–28. Nor do norms exist in contradistinction to law, whatever colloquial conceptions in diplomatic circles may suggest to the contrary. Laws (including international law) may be the basis for a norm just as an existing norm may eventually become instantiated in law. But many norms exist independently of law, just as some laws fail to realize their normative aspirations. Ibid., 441–42.

18 See Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1998): 887, 909–15.

19 See Finnemore and Hollis, "Constructing Norms," 456.

20 Katzenstein, "Alternative Perspectives on National Security," 5.

21 See Finnemore and Hollis, "Constructing Norms," 438–44.

22 Ibid., 440–41.

23 Ibid., 474.

24 See Finnemore and Sikkink, "International Norm Dynamics," 899; Finnemore and Hollis, "Constructing Norms," 468–69.

25 See, e.g., Amitav Acharya, "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism," *International Organization* 58 (Spring 2004): 239, 275; Richard Price, "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines," *International Organization* 52, no. 3 (July 1998): 613, 644.

26 Finnemore and Hollis, "Constructing Norms," 468–69.

27 Ibid., 474. For alternative typologies of the social processes by which norms work, see Ryan Goodman and Derek Jinks, *Socializing States: Promoting Human Rights through International Law* (New York: Oxford University Press, 2013), 4; Jeffrey T. Checkel, "International Institutions and Socialization in Europe: Introduction and Framework," *International Organization* 59, no. 4 (Autumn 2005): 801; Alastair Iain Johnston, "Treating International Institutions as Social Environments," *International Studies Quarterly* 45, no. 4 (2001).

28 See Finnemore & Hollis, "Constructing Norms," 453.

29 On the importance of context to norms, see Toni Erskine and Madeline Carr, "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace," in *International Cyber Norms: Legal, Policy & Industry Perspectives,* ed. Anna-Maria Osula & Henry Rõigas (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 87–88.

30 Finnemore and Hollis, "Constructing Norms," 427.

31 Eva Dou, "China's Xi Jinping Opens Tech Conference with Call for 'Cyber Sovereignty,' " *Wall Street Journal,* November 16, 2016, https://www.wsj.com/articles/chinas-xi-jinping-opens-tech-conference-with-call-for-cyber-sovereignty-1479273347.

32 A number of states have, for example, demonstrated some receptiveness to the idea of cyber sovereignty and the accompanying norm that states can and should have plenary control over the content of Internet traffic within their territories. See, e.g., Gerry Shih, "China seeks global support for cyber sovereignty framework," *Phys.org,*

March 2, 2017, https://phys.org/news/2017-03-china-global-cyber-sovereignty-framework.html. If successful, these norm promotion efforts may have significant implications for the United States' own promotion of the IL norm.

33 See, e.g., Daniel Bodansky, "Rules vs. Standards in International Environmental Law," *Proceedings of the American Society of International Law* 98 (2004): 275; Kathleen M. Sullivan, "The Supreme Court, 1991 Term—Foreword: The Justices of Rules and Standards," *Harvard Law Review* 106, no. 22 (1992): 57–59; Pierre J. Schlag, *Rules and Standards, UCLA Law Review* 33 (1985): 379. Separately, although I don't analyze it here, it is worth noting that norms may direct behavior in line with different functions, whether regulative (e.g., prohibitions, permissions, requirements) or constitutive (i.e., creating new actors or institutions). Finnemore and Hollis, "Constructing Norms," 469.

34 Recent scholarship has begun to offer an alternative definition of a norm that requires an identified group of actors to perform or refrain from certain specified actions. See, e.g., Michelle Jurkovich, "What Isn't a Norm? Redefining the Conceptual Boundaries in International Relations" (working paper on file with author, 2016): Michelle Jurkovich, "Boomerang or Buckshot? Blame Diffusion in International Hunger Advocacy" (unpublished doctoral dissertation, George Washington University, on file with author). Under this approach, we might differentiate norms and principles as separate concepts. Although an interesting idea, I do not follow it here, preferring the mainstream approach under which principles qualify as norms since they set sufficient—if still broad—behavioral expectations for their subjects.

35 See White House Press Secretary, "Fact Sheet."

36 For more on the idea that the question "who should do what" helps delineate norms, see Jurkovich, "What Isn't a Norm?"

37 Jack Goldsmith goes further and characterizes such precision in terms of loopholes. See Jack Goldsmith, "China and Cybertheft: Did Action Follow Words?" *Lawfare* (blog), March 18, 2016, https://www.lawfareblog.com/china-and-cybertheft-did-action-follow-words.

38 See Kenneth W. Abbott, Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter, and Duncan Snidal, "The Concept of Legalization," *International Organization* 54, no. 3 (Summer 2000): 401, 412–414.

39 Ibid.

40 See FireEye, "Red Line Drawn"; Iasiello, "Ramping Down Chinese Commercial Cyber Espionage"; O'Neill, "Chinese Hacking."

41 See Finnemore and Hollis, "Constructing Norms," 457, 467.

42 Ibid., 441.

43 See Dou, "Call for Cyber Sovereignty," and Shih, "China Seeks Global Support."

44 There is evidence that China has already conceded as much. See 2015 GGE Report.

45 For more on normative communities, see Finnemore and Hollis, "Constructing Norms."

46 I say "opting" here on the assumption that the United States had several paths for pursuing the formation and spread of the CCE norm. It is possible, however, that the existing contexts inside (and out of) the cyber diplomacy realm involved path dependencies or other constraints that limited the scope and number of available US options.

47 Finnemore and Hollis, "Constructing Norms," 465–66.

48 See "G-20 Leaders' Communiqué," Antalya Summit, November 15–16, 2015, ¶26, www.mofa.go.jp/files/000111117.pdf; Stefan Nicola, "China Working to Halt Commercial Cyberwar in Deal With Germany," *Bloomberg Technology,* October 29, 2015; Rowena Mason, "Xi Jinping State Visit: UK and China Sign Cybersecurity Pact," *The Guardian,* October 21, 2015, https://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron. Alternatively, it is possible that these results were (softly) coordinated by the United States and its Western allies in advance, which would make the choice of the CCE norm's identity actually more pluri-lateral than bilateral.

49 See, e.g., Elias Groll, "Spy vs. Spy, America and Israel Edition¸" *Foreign Policy,* March 24, 2015, http://foreignpolicy.com/2015/03/24/spy_vs_spy_america_and_israel_edition.

50 See Agreement on Cooperation in Ensuring International Information Security, Russia-China, April 30, 2015, No. 788-r.

51 See generally Alastair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton, NJ: Princeton University Press, 1995); Alastair Iain Johnston, "Cultural Realism and Strategy in Maoist China," in *The Culture of National Security: Norms and Identity in World Politics,* ed. Peter J. Katzenstein (New York: Columbia University Press, 1996).

52 Finnemore and Hollis, "Constructing Norms," 467.

53 Ibid., 472.

54 See Iasiello, "Ramping Down Chinese Commercial Cyber Espionage"; White House Press Secretary, "Fact Sheet."

55 Finnemore and Hollis, "Constructing Norms," 469–72.

56 Brendan Nicholson, "Bishop: We Don't Support a New Cyber Crime Treaty," *The Australian,* April 17, 2015 (quoting Chris Painter in Tolkienian terms: "We don't need a new treaty. . . . We don't need one ring to rule them all."); Waxman, "Self-Defensive Force," 115.

57 For more on the trade-offs between using treaties and political vehicles, see Duncan B. Hollis and Joshua J. Newcomer, " 'Political' Commitments and the Constitution," *Virginia Journal of International Law* 49 (2009): 507, 526; see also Jack Goldsmith and Eric A. Posner, *The Limits of International Law* (New York: Oxford University Press, 2006),91–100; Kal Raustiala, "Form and Substance in International Agreements," *American Journal of International Law* 99 (2005): 581, 592; Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organization* 54 (2000): 421; Charles Lipson, "Why are Some International Agreements Informal?" *International Organization* 45 (1991): 495.

58 Of course, the IL norm was promoted not in a legal, but in a distinctly political setting—the UN GGE.

59 See "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries," *Yearbook of the International Law Commission, 2001,* vol. 2, part 2, UN Doc A/56/10 (as corrected); Finnemore and Hollis, "Constructing Norms," 468.

60 See, e.g., Goldsmith and Posner, *Limits of International Law;* Harold Hongju Koh, "Why Do Nations Obey International Law?" *Yale Law Journal* 106 (1997): 2599, 2630–34.

61 See Martha Finnemore, "Are Legal Norms Distinctive?" *New York University Journal of International Law and Politics* 32 (2000): 699.

62 See, e.g., Hollis and Newcomer, " 'Political' Commitments and the Constitution," 526 (listing speed as one component of the flexibility offered by political commitments); Lipson, "Why are Some International Agreements Informal?" 500.

63 Department of Justice, "U.S. Charges Five Chinese Military Hackers with Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage" news release, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; Michael S. Schmidt and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times,* May 19, 2014, https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html.

64 *See* Samm Sacks, "China's Cybersecurity Law Takes Effect: What to Expect," *Lawfare* (blog), June 1, 2017, https://lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

65 Interestingly, the reduction in Chinese cyberespionage came in 2014 shortly after these indictments. It is not clear, however, whether that is because the indictments revealed to China the depth of an internal agency

slippage problem it was already incentivized to correct or because the negative incentives of the indictments themselves influenced China to accept the CCE norm. See Goldsmith, "China and Cybertheft."

66 See Goodman and Jinks, *Socializing States,* 180.

67 Finnemore and Hollis, "Constructing Norms," 472–73.

68 Ibid.

69 For more on attribution, see P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2015), 72–76; Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52, no. 2 (Summer 2011): 373, 397–401.

70 Finnemore and Hollis, "Constructing Norms," 443–4.

71 Ibid; Thomas Risse and Kathryn Sikkink, "The Socialization of International Human Rights Norms into Domestic Practices: Introduction," in *The Power of Human Rights: International Norms and Domestic Change,* eds. Thomas Risse, Stephen C. Ropp, and Kathryn Sikkink (Cambridge, UK: Cambridge University Press, 1999), 1, 17–35.

72 See 1975 Conference on Security and Cooperation in Europe: Final Act, State Department Bulletin 323, 73; see also Daniel C. Thomas, *The Helsinki Effect: International Norms, Human Rights, and the Demise of Communism* (Princeton, NJ: Princeton University Press, 2001); Finnemore and Hollis, "Constructing Norms," 443–4.

73 FireEye, "Red Line Drawn," 11 (charting the significant decline in commercial cyberespionage by seventy-two suspected China-based groups between February 2013 and May 2016); O'Neill, "Chinese Hacking."

74 Sunstein uses the example of religious liberty: people believe in it, but for very different reasons. Some favor it to preserve their own beliefs, some view religious freedom as a moral command, others accept its existence on utilitarian grounds, while still others see it in national security terms—i.e., as a way to preserve social peace. Cass R. Sunstein, "Incompletely Theorized Agreements in Constitutional Law," *Social Research* 74, no. 1 (Spring 2007). Sunstein's idea shares similarities with Rawls's concept of overlapping consensus. John Rawls, "The Idea of an Overlapping Consensus," *Oxford Journal of Legal Studies* 7, no. 1 (Spring 1987).

75 See 2015 GGE Report (citing sovereignty as a relevant area of international law).

76 FireEye, "Red Line Drawn," 5.

77 See O'Neill, "Chinese Hacking," (quoting US Director of National Intelligence Dan Coats: "Beijing has also selectively used offensive cyber operations against foreign targets that it probably believes threaten Chinese domestic stability or regime legitimacy").

78 See Acharya, "How Ideas Spread"; Price, "Reversing the Gun Sights."

79 Ibid.

80 There were also several, less formal Track 2 diplomatic efforts. See Greg Austin, "International Legal Norms in Cyberspace: Evolution of China's National Security Motivations," in Osula & Rõigas, *International Cyber Norms,* 194–95.

81 See, e.g., Nazir Kamal, "Group of Governmental Experts on UN Register of Conventional Arms Concludes Headquarters Session, Adopts Consensus Report," news release, United Nations, August 1, 2003, www.un.org/press/en/2003/dc2880.doc.htm.

82 See, e.g., Korzak, "International Law and the UN GGE Report"; Fidler, "The UN GGE on Cybersecurity"; Marks, "U.N. Body Agrees to U.S. Norms"; Segal, "UN's Group of Governmental Experts"; Australian Department of Foreign Affairs and Trade, "Australia Welcomes UN Cyber Report," news release, August 14, 2013.

83 For more information on the First Committee's goals, see "Disarmament and International Security," First Committee, General Assembly of the United Nations, www.un.org/en/ga/first/, accessed April 5, 2017.

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

85 See, e.g., Mo Hong'e, "Third China-U.S. Cybersecurity Ministerial Dialogue Yields Positive Outcomes," *Xinhua,* December 9, 2016, http://news.xinhuanet.com/english/2016-12/09/c_135893317.htm; Mo Hong'e, "China, U.S. to Jointly Fight Cybercrime," *Xinhua,* June 15, 2016, http://news.xinhuanet.com/english/2016-06/15/c_135437030.htm; Chen Weihua, "China, US Talk Cyber Standards," *China Daily,* May 12, 2016, http://usa.chinadaily.com.cn/world/2016-05/12/content_25240147.htm; "China, U.S. Hold 1st Ministerial Dialogue on Cyber Security," *Xinhua,* March 12, 2015.

86 So far, however, the Trump administration has signaled a willingness to continue the Obama administration's cybernorm promotion efforts. See Thomas Bossert, "Next Steps for Cybersecurity After a Decade of Lessons Learned," speech, Cyber Disrupt 2017 conference, Center for Strategic & International Studies, March 15, 2017, https://www.csis.org/analysis/cyber-disrupt-2017-keynote-next-steps-cybersecurity-after-decade-lessons-learned.

87 See Anna-Karin Hatt, "A Multi-stakeholder Model for Prosperity," speech, Stockholm Internet Forum, May 27, 2014, www.stockholminternetforum.se/the-opening-address-by-anna-karin-hatt.

88 See, e.g., Samm Sacks, "Cybersecurity Won't Be the Biggest Deal at China's World Internet Conference," *Fortune,* December 15, 2015; "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 General Assembly, document A/69/723.

89 See Finnemore and Hollis, "Constructing Norms," 449.

90 See, e.g., Tami Abdollah, "U.S. Official Says China Should Pay Price If It Breaks Deal to Curb Economic Cyber Espionage," *U.S. News & World Report,* November 10, 2015, https://www.usnews.com/news/politics/articles/2015/11/10/us-official-china-should-pay-price-if-it-breaks-agreement; Department of Justice, "U.S. Charges Five Chinese Military Hackers"; Ellen Nakashima," U.S. Developing Sanctions against China over Cyberthefts," *Washington Post,* August 30, 2015, https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html?utm_term=.233b5c1bcdc3.

91 See Jack Goldsmith, "Thoughts on White House Pledge to Respond to DNC Hack," *Lawfare* (blog). October 12, 2016, https://www.lawfareblog.com/thoughts-white-house-pledge-respond-dnc-hack; David E. Sanger and Nicole Perlroth, What Options Does the U.S. Have after Accusing Russia of Hacks*? New York Times,* October 8, 2016, https://www.nytimes.com/2016/10/09/us/politics/what-options-does-the-us-have-after-accusing-russia-of-hacks.html.

92 See Iasiello, "Ramping Down Chinese Commercial Cyber Espionage."

93 See, e.g., James A. Lewis, "US–China Cyber Relations: Not a New Cold War," *The Strategist,* November 12, 2014, https://www.aspistrategist.org.au/us-china-cyber-relations-not-a-new-cold-war; *The Economist,* "Admit Nothing."

94 See Finnemore and Hollis, "Constructing Norms," 475.

95 FireEye, "Red Line Drawn," 3.

96 See Sunstein, "Incompletely Theorized Agreements"; Rawls, "Overlapping Consensus"; 2015 GGE Report; FireEye, "Red Line Drawn,"5.

97 Finnemore and Hollis, "Constructing Norms," 475.

98 See Tang Lan, "National Sovereignty Applies to Cyberspace," *China Daily,* April 20, 2016, http://usa.chinadaily.com.cn/opinion/2016-04/20/content_24681619.htm.

99 Finnemore and Hollis, "Constructing Norms," 475.

100 It is worth noting that the categories identified here are ideal types. Material incentives like sanctions have a naming-and-shaming function in the same way that—especially for particularly tight groups—the social sanction of naming and shaming may operate like a material incentive. Ibid., 475–76.

101 See, e.g., Nicole Perlroth, "Hackers in China Attacked the Times for Last 4 Months," *New York Times,* January 30, 2013, www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html; Department of Justice, "U.S. Charges Five Chinese Military Hackers."

102 Finnemore and Hollis, "Constructing Norms," 475–76.

103 Ibid.

104 Ibid., 476.

105 Tom Risen, "China, U.S. Work to Further Cybersecurity Pact," *U.S. News & World Report,* December 3, 2015, https://www.usnews.com/news/articles/2015/12/03/hotline-bling-china-us-work-to-further-cybersecurity-pact.

106 Austin, "International Legal Norms," 194–95. For more on how different states have different traditions of international law, see, for example, Anthea Roberts, "Is International Law International?" (Oxford, UK: Oxford University Press, forthcoming); Ugo Mattei, "Comparative International Law," *Brooke Journal of International Law* 36 (2001): 385.

107 The most renowned illustration of this phenomenon is the Israeli Day Care experiment. Researchers showed that imposing a fee for parents who picked up their children late from day care socialized those parents into thinking of the fine as a "price" for child care rather than a "penalty" for bad behavior. As a result of the fine, parent tardy pickups actually increased. Uri Gneezy and Aldo Rustichini, "A Fine Is a Price," *Journal of Legal Studies,* no. 1 (January 2000).

108 Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," Hoover Institution, June 2, 2017; see also 2015 GGE Report, ¶28(f).

109 Such a framework may also assist the United States in deconstructing—and responding to—norm promotion efforts by China or other actors.

110 Finnemore and Hollis, "Constructing Norms," 454–55.

111 Even fully internalized norms will evolve as issues of identity and notions of propriety change in both subtle and, sometimes, profound ways.

112 Depending on who one asks, espionage either lies entirely outside international law or is granted an exceptional status within the law (meaning that the law can dictate the shape of such an exception). See generally A. John Radsan, "The Unresolved Equation of Espionage and International Law," *Michigan Journal of International Law* 28, no. 3 (2007): 595, 603–7 (citing authors claiming espionage is legal, illegal, or neither legal nor illegal).

113 Of course, just as individual norm processes involve trade-offs, so too do larger projects seeking to construct sets or systems of norms. In this respect, US efforts to promote cybernorms with China must be cognizant of other cybernorm projects, let alone norm efforts in other areas (e.g., privacy, the environment).

The preferred citation for this publication is:
Duncan Hollis, **China and the US Strategic Construction of Cybernorms: The Process Is the Product**, Hoover Working Group on National Security, Technology, and Law, Aegis Paper Series No. 1704 (July 7, 2017), available at https://lawfareblog.com/china-and-us-strategic-construction-cypernorms-process-product.

About the Author

DUNCAN B. HOLLIS

Duncan B. Hollis is James E. Beasley Professor of Law at Temple University Law School. He is editor of the award-winning Oxford Guide to Treaties (Oxford University Press, 2012) as well as various articles on securing cyberspace, including (with Martha Finnemore) *Constructing Norms for Global Cybersecurity,* 110 American J. Int'l Law 425 (2016). Professor Hollis is a Non-Resident Scholar at the Carnegie Endowment for International Peace, an elected member of the American Law Institute, and a member of the OAS Inter-American Juridical Committee.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cyber security, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION