Norms and Normalization

Dr. Martin C. Libicki

The search for norms has proven to be one of the most frustrating elements of cyberspace operations. Informed consensus holds that there *should* be norms of international behavior to tame the Wild West of cyberspace. Yet, if norms are defined to exist when a country refrains from operations otherwise in its interest[1] (taking domestic and international politics into account) they do not exist. That is, there are zero such norms that enjoy adherence that matters.

In light of such disappointments, this paper mulls a different approach to thinking about norms. Rather than focusing on what responsible governments should *not* do, it looks at what they actually do as a guide to what activities in cyberspace have effectively been normalized (that is, within *de facto* norms)—and may remain normalized until the rewards from such activities no longer merit the effort.

This argument has three parts. The first part discusses the lack of progress towards norms. The second defines normalization and examines the extent to which the behaviors of specific countries establish what has, in effect, been normalized. The third part focusses on one particular activity—implanting malware into the weapons systems of potential adversaries—as a candidate for normalization.

FROM NORMS

Norms can be understood as rules for behaving that forbid or encourage[2] certain activity. As with information technology standards[3] anyone can propose a norm, but to be a successful norm requires that some critical mass of countries adhere to them.

Proposed norms for cyberspace have come from many sources. Three include an extension of the Laws of Armed Conflict (LOAC) from the physical world to cyberspace; negotiations among multiple states; and bilateral agreements, notably the Xi-Obama agreement of September 2015.

The proposition that LOAC applies in the virtual world as it does in the physical world would seem to be self-evident. Strictures on violations of sovereignty, the use of disproportionate force, gratuitous attacks, perfidy, the violation of neutrality, and so on rest on the belief in fundamental human rights and are therefore medium-agnostic. The Tallinn Manual[4] epitomizes the LOAC approach. Its technical quality is undeniable. Unfortunately, its scope is quite limited. International humanitarian law (of which LOAC is a component) aimed to modulate death, injury, and destruction from war. Cyberattacks, by contrast, have yet to hurt anyone directly, and very rarely break things in the physical sense. Their toll is measured in time and money, both of which fall outside the scope of LOAC. Granted, the second version of the Tallinn Manual[5] discusses countermeasures: what one state can do to make another state stop behaviors that levy time and money costs. But a broad right to self-defense allows certain behaviors; it does not forbid unwanted behavior. As for cyberespionage, which is far more common, the Tallinn Manual is silent. Conventional espionage does not fall under LOAC. Thus, ditto for cyberspace espionage—even though the distinction between conventional espionage and armed attack is far clearer than between cyber espionage and cyberattack.

Attempts to craft norms specific for cyberspace have not fared much better. The most official such endeavor is the U.N. Group of Government Experts (GGE). The high-water mark was the 2013 agreement among participating countries (notably the United States, Russia, and China) that LOAC covered cyberspace. But no sooner had Russia's and China's diplomats returned home than both governments concluded that even so simple an agreement was not really what they had in mind. Subsequent GGE sessions fared worse. Although the process revived[6] in 2019, expectations should be tempered. The closest to a formal norm for cyberspace—in the sense that it is a formal treaty that has been implemented in national law—comes from the Convention on Cybercrime of the Council of Europe (aka the Budapest Convention). It binds members to mutual assistance for cybercrimes. It works well within the group of signatories (e.g., by facilitating the arrests of cyber-criminals), but Russia and China are prominent among the non-signatories, and Russia, in particular, has shielded cyber-criminals from prosecution.[7]And the Convention imposes no restrictions on what *states* can do in cyberspace. Other initiatives to establish norms include those by Microsoft[8] and the Paris[9] declaration. Nice words by states and institutions that never had a desire or willingness to carry out problematic operations in cyberspace are no substitute for actual restraint shown by states that could and often do carry out such operations.

The closest workable norms in cyberspace arose from the personal agreement between President's Xi of China and Obama of the United States (US) to cease cyberespionage against commercial firms for commercial purposes (but bypassed activities such as hacking commercial firms to find exploitable flaws in their products or looking for records of terrorist activity). This agreement was extended globally in a subsequent G20 agreement[10]. For the first time, a major country had agreed to stop doing something that clearly benefitted it. Alas, while the agreement initially reduced China's cyber-espionage, Chinese cyberespionage levels[11] apparently

reverted to form in early 2017. The primary difference between then and now is that operators are more discreet in their techniques and target selection.

Two problems bedevil effective norms-making in cyberspace. One would be difficulties in attribution; they allow governments to advocate for restrictions they violate in the belief that can plausibly deny. Granted, rarely does a major cyberattack takes place without one or more cybersecurity companies (and increasingly, governments) assigning blame. Their assessments are usually credible. But the process by which cyberattacks are attributed is opaque and often bereft of details. Governments are particularly reluctant to explain their rationale for their judgments, particularly when they have used sensitive sources and methods to draw conclusions. As a result, those inclined to be skeptical can maintain their doubts. Countries can and do blandly assert that accusations against them arise from animus, not evidence. In fairness, once cases get to court, the evidence is presented and prosecutions often result. Since 2014, the US has been energetic in issuing indictments[12] against state-hired or at least state-supported actors, suggesting it has similar evidence, but none so indicted have appeared in court.[13] Increasingly, it seems, your friends will believe your facts and your foes will not. This is not an environment in which good behavior results from fear of credible accusations.

A more significant problem may be that the desire for norms is asymmetric. They are seen as signifiers imposed on misbehaving countries by those who see themselves virtuous. Take the Xi-Obama agreement. China forewent operations that profited them; the US forewent operations that it had no interest in—while giving itself a pass on those types of cyber-espionage against commercial that *did* interest them. There was no comparable behavior from the US that China both wanted to modulate and had a reasonable prospect of so doing in return. No US administration, for instance, could credibly promise to squelch the free speech of dissidents. As a rule, countries agree to asymmetric deals only under coercion. In the Obama era, the threat was sanctions. The Trump Administration, however, signaled that the Chinese were engaged in a large variety of "unfair" trade practices, not just intellectual property theft. Sanctions would, therefore, be coming irrespective of China's conformance with the Xi-Obama deal. So, why keep its terms? The broader rule applies: norms established in state-to-state negotiations require proponents to give up something as well as receive if such norms are to persist.

From the US (or broadly Western) perspective, matters are unlikely to improve. Relations with Russia turned sour in 2014 (as a result of Crimea). Relations with China did likewise in 2017 (as a result of trade disputes). Disunity in the West has made it harder to reach internal agreement on norms, much less apply unified coercive pressure. It does no good to plead that civilized Western states have advocated and adopted a set of norms-like practices. For the most part, they are not each other's targets in cyberspace. But the West, in general, does compete with countries such as Russia or China—and to recognize as norms those activities which the West has or would like to abjure is akin to asking for unilateral disarmament hence, not viable.

TO IMPLICIT NORMALIZATION

Consider now a different approach, concentrating on normalization rather than norms. Norms say what states should not do. Normalization says that certain activities are regarded as part of the given environment and likely to stay that way, either because they are deemed legitimate state behavior or because there is no reasonable prospect that they will end. An example of normalized behavior was the Soviet practice of parking trawlers near U.S. naval exercises in open waters (largely to facilitate eavesdropping). The US initially objected to this practice, but when the Soviets proved adamant that their behavior was permitted and not harmful, the US grudgingly accepted this as a normalized state of affairs[14] Indeed, the impetus for objecting to this or that behavior is often that if it remains undisputed, it will become normalized. British Foreign Secretary Jeremy Hunt's praise of EU cyber sanctions was based on the hope that "We can now impose tough sanctions on those responsible for malicious cyber-attacks. [Otherwise] trying to interfere in other countries' democratic processes is becoming normalized."[15]

Explicit normalization also helps make the case for norms. As Max Smeets has observed[16] of the US: there are many practices that raise objections, but few, if any, that are deemed acceptable and will not be challenged. Normalization of some practices makes norms against other practices seem reasonable rather than as a list of generalized complaints. It distinguishes between the permissible and the impermissible.

Putatively, norms and normalization should be like a mold and a casting: the existence of one implies the other because everything is either allowed or it is not. Unfortunately, it is nearly impossible to create a definitive list of cyber operations that can be so evaluated. Surprises—not only what states *would* do but what states *could* do—keep coming. In 2015, when members of the Defense Science Board—a savvy group—tried to enumerate what behavior would cross a US red line, not one of them suggested something like the 2016 DNC hack. But normalization would at least suggest what buckets various operations could fall into.

One example of normalized behavior is that countries are allowed to carry out cyberespionage in support of national security decision-making (much as conventional espionage is considered normalized state behavior). Roughly speaking, an activity is normalized when carried out by at least one capable and serious country—especially if that country does not deny such activity (admitting to such activity is a less realistic prospect) or make excuses about it. This hardly means that other countries accommodate such practices. In many cases, they will object. But if such objections fall on deaf ears and more forceful responses elicit only countervailing pressure by the accused state, then at some point others will concede that such practices are here to say, and maybe they, themselves, should adopt them. Thus, even if the point is to establish behavior for the other side to negotiate away, for example, another state may adopt a practice that the first state would rather not see. Others also do so. The initiating state may then conclude it would be better off in a world in which such practices were foresworn.

So, *which* country's activities can credibly establish the norms for the rest of the world?

Start with two that would not. North Korea has carried out severely disruptive cyberattacks against targets in South Korea and the Sony Corporation. Its hackers have robbed banks, most notably the central bank of Bangladesh, as well as several digital currency exchanges.[17] To set North Korea as the standard for normalization essentially normalizes bank robbery. Similarly, Iranian hackers have trashed computers (notably those of Saudi Aramco and Las Vegas Sands Corporation); worse, they have been implicated in tampering with safety systems in industrial facilities. Again, to set Iran as the standard would normalize highly dangerous practices. That North Korea and Iran have essentially put themselves on a war footing (vis-à-vis South Korea and Saudi Arabia, respectively) may excuse them. Yet, it hardly normalizes behavior for countries that are not on a war footing.[18]

Russia presents a problem because it is too big (and too adept in the arts of cyberspace) to be dismissed as a basis for normalization. But Russia's behavior, at least since late 2013, has crossed limits (i.e., taking territory from a neighboring country) that had been adhered to by the Soviet Union once World War II was over. As for cyberspace operations, Russian hackers have interfered in the politics of the US, the United Kingdom, and several other countries. Russian hackers are believed by the U.S. Intelligence Community (IC) to have implanted malware in the electrical grid of the US[19] and Europe. Russian hackers have corrupted the software and knocked offline the power grid of a state in peacetime. Thus, using Russia as the standard for normalization would require accepting that such activities can be expected from responsible countries. This is broadly unacceptable, not least to the US.

One problem with normalization is apparent in the above: these are all activities that have been attributed to Russia but never acknowledged.[20] This could present difficulties if Western countries did the same to others, notably Russia, and excused their activities by arguing that Russia's behavior had *de facto* normalized such operations—only to be met by denials that Russia had done what it was accused of. But if Russia *were* to object to cyberspace operations against it, carrying the objection puts the burden of proof on its own shoulders. Arguing that China did it would not dent the West's view that such activities were normalized, it would only shift the blame.

China presents a better case that its behavior can set the standard for what can be considered normalized. Its economy is putatively the world's largest, its population undoubtedly so, and it is increasingly adept at cyberspace operations. In contrast to North Korea, Iran, and Russia, all of whom are trying to upset the world order, China is content with the structure if not necessarily the leadership of the world order. Although China has carried out a great deal of cyberespionage, its *known external* cyberattack activity has been limited to DDOS attacks on dissidents (and dissident-used Web sites such as GitHub). But to accept Chinese behavior as normalized means accepting cyberespionage for commercial purposes, something that China has formally foresworn. And it is difficult to believe that the many BGP (border gateway proto-

col) attacks[21] ascribed to China have all been accidents—although, if deliberate, their purpose has been for cyberespionage which itself is largely normalized. Nevertheless, would the West be comfortable if China's behavior *were* the rules of the road?

Before getting to the putative gold standard for cyberspace normalization, it would help to go over the limits of normalization. Normalization does not mean that every country does as much as they are capable of (even if that is a serious constraint on mischief in cyberspace). Countries can abjure operations for political and strategic purposes. Some operations would sit poorly with their polities. Also, many who have advocated against certain practices would be taking risks if they conceded that their words avail naught and do what they have condemned – without at least a nod to their changing standards. Furthermore, just because Russia and China behave in cyberspace in ways that violate what the West would like to see as norms does not mean that they do not operate under their own restraints, perhaps in the hopes that the West would someday follow suit. That said, it is unclear what they refuse to do because it is wrong *vis-à-vis* because it might backfire.

That brings us to the US. Its size, sophistication, and alliance structure all suggest it alone normalizes behavior in cyberspace. Furthermore, the US has, among the powers, been most vociferous in advocating for norms of responsible state behavior in cyberspace, which means that if the US does something, it is unlikely that the US would advocate for its not being done. Finally, although the US does not own up to everything it is accused of, outright false denials are quite rare, particularly in the post-Snowden era.[22] To wit, whether it wants to or not, US behavior has become the gold standard.[23]

What might be considered now-normalized behavior because the United States has already done it?

First, the US has, in all likelihood, carried out cyberattacks designed to impede the production of nuclear weapons and their delivery systems. Stuxnet is an example of the first: it was used against Iran, and maybe against North Korea (albeit with no known effect[24]). Reportedly, the US tried to interfere with North Korea's production of reliable liquid-fueled intermediate-range missiles.[25] So, is breaking other people's weapons behavior that merits normalization? Or are nuclear weapons, in their destructiveness and appeal to rogue regimes, special enough to belong in their own category? Perhaps using cyberspace operations to break the nuclear weapons systems of proliferators can be considered normalized behavior – without necessarily extending the practice to *accepted* nuclear powers[26] (e.g., China) or other frightening weapons (e.g., hypersonic missiles).

Second, although cyberespionage against individuals is as acceptable state practice as is espionage against them, the US reportedly has surveilled a large body of communications in order to select the handful that represents people of interest.[27] In a sense, this echoes how it works with traditional radio-frequency signals intelligence – as well as with Defense Advanced Research Projects Agency's (DARPA) proposed Terrorist Information Awareness. Five to ten

years ago, the Chinese might have objected to such normalization, but their theft of U.S. Office of Personnel Management (OPM) data to (reportedly) find US espionage agents and help recruit their own, coupled with breaches of airline companies (e.g., United and American), health insurers (Primera, and Anthem), hotels (Marriott), and contractors who work personnel clearance (USIS) suggests that they view harvesting hay in pursuit of needles as normalized state behavior.

Third, recent claims of USCYBERCOM activity could normalize new categories of cyberspace operations. One is persistent engagement. Although the specific operation claimed in the press—a DDOS attack to stymie Russia's Internet Research Agency[28]—was small potatoes, it is unlikely to be the only such engagement. Accordingly, one must presume that cyber operations meant to interfere with cyber operators on the other side is fair game (even if many of these cyber operators are carrying out cyberespionage, which is a normalized activity). The modest risks of escalation, and the nature of cyberwarrior-on-cyberwarrior combat, aside, this development does not seem to be particularly problematic. The targets have little cause to complain.

Fourth, in early June 2019, the *New York Times*[29] reported (apparently without pushback from DoD) that USCYBERCOM was stepping up its efforts to insert malware into the Russian grid. This would supposedly deter Russia's activating the malware suspected to lurk in the US grid.[30] If true, it signals that the US regards implants in electric grids as already having been normalized by Russian behavior—and that the Administration had too little confidence that the Russians could be persuaded to withdraw their implants or abjure from implanting more malware (although, as with nuclear weapons, the practice of implanting malware can, in theory, be de-normalized by subsequent treaty). Perhaps needless to add, once malware is implanted nothing prevents its use in an opening salvo or being brandished as a deterrent against other unwanted behavior. Of note is that, as a GGE member, the US had agreed that the peacetime use of cyberattacks against critical infrastructure is out of bounds; thus, either such agreement is void, or the presumption now is that Russian cyberattacks against the electric grid are *de facto* acts of war. Again, if press reports of *Nitro Zeus* are correct,[31] the US had pre-wired Iran's electric grid *before* reports surfaced that Iran had done the same to the US grid.[32]

Fifth, in the days after a U.S. Global Hawk was shot down by Iranian batteries, the US purportedly[33] carried out cyberattacks. Using cyberattacks as a tit-for-tat would appear to be itself unexceptional and does not normalize cyberattacks except against something that looks close to armed conflict. But, if it takes weeks and more likely months to prepare such an attack,[34] then these implants *preceded* the Iranian attack. Therefore, the US has signaled its right to lay in attacks against military systems of potential adversaries in peacetime. Was this deliberate? It may have resulted from the calculation that the US has more to gain than lose from opening that door. If implants are limited to military systems, rather than extended to dual-use systems, the risk to civilians is limited. Doing so potentially substitutes nonlethal for lethal means of combat. It may have reflected a perception that potential adversaries of the US are unbound

by norms, and thus, why not prepare the cyberspace battlefield if the alternative is to accept a military disadvantage? Or, as per human nature, actions come first and wondering if such actions changed the rules of the game come later.

AND EXPLICIT NORMALIZATION

Now, go one step further. Perhaps the US should explicitly declare that preparing the battlefield through injected implants into (or using comparable means such as credentials hijacking or placing physical devices near to) potentially hostile defense systems is a legitimate state activity. In that sense, such peacetime activity is no less legitimate than is preparing the conventional battlefield through remote surveillance.

Note that announcing that implants are legitimate state activity and inserting implants are two different actions. One can be done without the other. The first essentially says to potential adversaries that the US could be in your military systems in ways that make them malfunction, create safety hazards associated with combat use (creating hazards for peacetime exercise use is a hostile activity), or, at very least, creating telemetry data when they are used (the better to target them with precision weapons). Others may dismiss these claims: Russia[35] and Iran[36] both deprecated reported claims to have interfered with their systems. But behind such public sang-froid must lie some degree of concern on the target's part, which at very least will complicate its war planning. Indeed, while military systems fail statistically in combat, the prospect that every weapon of a particular class may fail in a very public matter at the outset of aggression cannot help but temper the confidence that aggressors must feel before they start to war. The prospect of embarrassment may be more daunting than the prospect of defeat. Conversely, such an advantage may be temporary given the contest between measure and countermeasure. In practice, as well, the credibility of an assertion that the US is in the systems of others may require demonstration from time to time. And while the failure to complete an implant may go unnoticed, the failure to exercise an implant in circumstances where others expect it (i.e., when the US has an interest in seeing systems fail then and there) may erode credibility.

The value of such an announcement may also lie in what happens when an implant is discovered in someone else's military system. Under current circumstances, the victims could easily conclude that the implant itself means that combat is coming, and probably soon—ignoring that implantation may have preceded discovery by months and years. Such conclusions may give rise to thoughts of pre-emption.[37] However, if the US has explicitly indicated that it would, where possible, insert implants in potential adversary systems as day-to-day practice, the discovery of an implant should be less likely to point to imminent conflict. Furthermore, while discovery may indicate that inserting implants is not risk-free, it could also signify that the US talk about implants are not mere words.

The last argument returns us to the problem of norms. As argued above, one reason that the Xi-Obama agreement on cyberespionage is ailing is that it was not a trade in which both parties gained but one made under a one-sided threat and only as good as the threat lasted.

To the extent that other countries fear the US loading implants into military systems works in that they may be amenable to norms in which they give up something they want to do if the US does likewise. They would be inhibited from backsliding by the fear that the US would return to practices they, themselves, disliked.[38] Perhaps needless to add, attribution issues will face both sides in such a trade. Furthermore, if US cyberwarriors see serious advantage in implantation, they will be reluctant to trade it away (especially for norms without military implication: e.g., against vote-tampering). It would not be the first time that organizations fell in love with their bargaining chips.

A tricky issue may also arise if other countries believe that US cyberspace activities extend to their far more consequential nuclear systems. One need not imply the other. Normalizing implants in conventional military systems is far different from normalizing them in nuclear systems in general or nuclear command-and-control systems in particular. Countries nervous about the viability of their nuclear deterrent can react in ways that make nuclear war—notably inadvertent or accidental nuclear war—more likely. But would a US statement that it would differentiate between conventional and nuclear systems assuage them? In some countries, the two types of systems are entangled.[39] But even where they are not, simply introducing the prospect of implants may spark fears that could override distinctions that are later offered.

Would declaring an open season for implants on conventional military systems work to the US advantage? Although U.S. cyber operators are second to none, the U.S. military has also embraced digitization and networking far more than others have. Nevertheless, an explicit declaration may remove constraints on USCYBERCOM while having little effect on adversaries who are unbothered by US views on norms. And, such a declaration may not be so far from current practice even among U.S. allies. Florian Kling, who leads a German military watchdog group, holds

> that international law allows for preemptive attacks in self-defense if a military strike is imminent, but not preventive attacks; cybersecurity operations lie somewhere in between. 'We would have to identify gaps in their security and implant a Trojan or virus so that the next time they attack, we can shut down their system … and therein lies the problem: Is that a preemptive strike, if the opponent hasn't yet attacked or initiated any actions?[40]

There are other sources of caution. With such a declaration, the US loses the ability to hold other countries to account when they infiltrate US systems. Even if the US comes out ahead by opening the arena, U.S. allies—many with far fewer offensive cyberspace capabilities—may lose more then they gain if defense systems become fair game for implants. Would purchasers of US defense products conclude that the normalization of implants in an adversary extends to legitimizing kill-switches in such products (that could be activated in case of misuse or a change in government orientation)? And, finally, there is no guarantee that others will strictly adhere to the same definition of what is normalized. Can the US declare that defense systems are inbounds for implants but that dual-use infrastructures (e.g., electricity, telecommunications)

are not—only to find that other countries conclude that implants on the latter are normalized by the same logic? Would such normalization suggest that implants in police and/or surveillance systems of other countries are also legitimate extensions of allowing implants into their military systems? If the US normalizes implants but does not normalize their activation except in times of war, would other countries adhere to the same notions of what constitutes war that the US does?

That noted, the admonition not to move thoughtlessly is not the same as the admonition not to move.

CONCLUSIONS

Norms are ideals. Normalization concedes that states do not run on ideals. In theory (and some practice), the West has been promoting ideals to foster a world in which the rule of law rather than the Melian dialogue is a guide to international behavior. But behind these ideals have been countries whose strength—military, but also economic (see sanctions)—helps ensure that these ideals are put into practice. There is no *ipso facto* reason why cyberspace should not be subject to the rule of law, even—perhaps especially—as they affect responsible state behavior. But realistically, after a quarter-century of interest and at least ten years of real work, progress has been disappointing. 2015 appears to have been the high-water mark for the ability of norms to curb unwanted state behavior.

Normalization is the recognition that states will continue to do things in cyberspace, not necessarily to the advantage of other states. But by concentrating not on what is forbidden but by what is permitted through common practice, it is possible to reason by exception to see what the feasible space of norms may be. It grounds the search for norms in *realpolitik* that correctly reflects the ambiguities of activity in cyberspace, and the license it gives actors. Explicit normalization may play a role in this process. In the case presented above, a declaration that military systems may not be considered safe from implants provides many advantages and may spur other countries into taking norms (and concomitant attribution challenges seriously).

Author Bio

Dr. Martin C. Libicki

Martin Libicki (Ph.D., U.C. Berkeley 1978) is the MaryEllen and Richard Keyser Chair of Cybersecurity at the U.S. Naval Academy where he teaches cyberwar strategy and cyberspace economics. Prior employment includes having been a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. He wrote three commercially published books: *Cyberspace in Peace and War* (2016, second edition forthcoming), *Conquest in Cyberspace: National Security and Information Warfare* (2007), and *Information Technology Standards* (1994). He is also the author of numerous RAND monographs, notably Defender's Dilemma, Brandishing Cyberattack Capabilities, Crisis and Escalation in Cyberspace, Global Demographic Change and its Implications for Military Power, Cyberdeterrence and Cyberwar, How Insurgencies End (with Ben Connable), and How Terrorist Groups End (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

NOTES

1. In theory, a state could believe that operation X was to its advantage if its foes did likewise – but not to its advantage if its foes also abjured. So, *other countries'* restraint would not change the underlying fact that the state was optimizing without regard to norms. Plausible examples of this in cyberspace are not easy to find, especially because it is often unclear what one's foes are, in fact, doing in cyberspace.
2. One example of a proposed rule to encourage good behavior is Duncan Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal*, Volume 52, Number 2, Summer 2011, 374-432.
3. On standards, see, for instance, Martin Libicki, *Information Technology Standards: Quest for the Common Byte*, Digital Press, 1995.
4. For the first version, see the *'Tallinn Manual' on the International Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence DRAFT (as of August 21, 2012).
5. Michael Schmitt et al, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," Cambridge UK (Cambridge University Press), 2017.
6. Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," November 15, 2018; https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
7. E.g., see Nicole Perlroth, "Online Security Experts Link More Breaches to Russian Government," October 28, 2014; https://www.nytimes.com/2014/10/29/technology/russian-government-linked-to-more-cybersecurity-breaches.html or Mark Johnson, "Russia Issues Travel Warning About US, Citing Threat Of 'Kidnapping'", IB Times, September 3, 2013, http://www.ibtimes.com/russia-issues-travel-warning-about-us-citing-threat-kidnapping-1402265.
8. Scott Charney *et al, From Articulation to Implementation: Enabling progress on cybersecurity norms*, June 2016.
9. *The Paris Call for Trust and Security in Cyberspace*, December 11, 2018; https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.
10. For a copy of the communique and a discussion thereof see Cody Poplin, "Cyber Sections of the Latest G20 Leaders' Communiqué," November 17, 2015; https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communiqué.
11. Adam Segal *et al, Hacking for CaSh: Is China Still Stealing Western IP?*, September 24, 2018; http://apo.org.au/node/194141.
12. Against China, see Ellen Nakashima, "Indictment of PLA hackers is part of broad U.S. strategy to curb Chinese cyberspying," Washington Post, May 22, 2014, http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html; against Russia see "United States v. Viktor Borisovich Netyksho et al," Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18; https://www.justice.gov/file/1080281/download; against Iran see From Ellen Nakashima and Matt Zapotosky, "U.S. charges Iran-linked hackers with targeting banks, N.Y. dam," March 24, 2016; https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html.
13. The arrest and conviction of Karim Baratov is the closest to an exception; see David Shepardson, "Canadian who helped Yahoo email hackers gets five years in prison," May 29, 2018; https://www.reuters.com/article/us-yahoo-cyber/canadian-who-helped-yahoo-email-hackers-gets-five-years-in-prison-idUSKCN1IU2OE.
14. See David Frank Winkler, *The Cold War at Sea: High-Seas Confrontation Between the United States and the Soviet Union* (Annapolis, Md.: Naval Institute Press, 2000).
15. See Joseph Marks, "The Cybersecurity 202: These political candidates are running on their cybersecurity expertise," May 20, 2019; https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/20/the-cybersecurity-202-these-political-candidates-are-running-on-their-cybersecurity-expertise/5ce20017lad2e54b957e7fb2/.
16. Max Smeets, "There are Too Many Red Lines in Cyberspace," March 20, 2019; https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace.
17. Matt Burgess, "North Korea's elite hackers are funding nukes with crypto raids," April 3, 2019; https://www.wired.co.uk/article/north-korea-hackers-apt38-cryptocurrency.
18. A similar argument can be made for Israel, which has carried out physical attacks in Syria and has been implicated in assassinations in Iran. Israel, technically and in some aspects practically, is at war with its neighbors. Again, such a justification means that its actions do not normalize operations in cyberspace for countries at peace.
19. Lily Hay Newman, November 28, 2018; "Russian Hackers Haven't Stopped Probing the US Power Grid," https://www.wired.com/story/russian-hackers-us-power-grid-attacks/.

NOTES

20. President Putin has compared those who hacked the DNC to "artists." See Andrew Higgins, "Maybe Private Russian Hackers Meddled in Election, Putin Says," June 1, 2017; https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html.
21. Chris Demchak, Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," Military Cyber Affairs, 3:1 (2018).
22. See, for instance, Scott Shane and Jonathan Weisman, "Earlier Denials Put Intelligence Chief in Awkward Position," June 11, 2013; https://www.nytimes.com/2013/06/12/us/nsa-disclosures-put-awkward-light-on-official-statements.html.
23. Considering oneself the gold standard has one obvious disadvantage. Any U.S. decision to do something that has never been done raises the question of whether doing so would give other the green light to do likewise. It is hard to believe that North Korea, Iran, Russian, and (for the time being) China make similar calculations.
24. Joseph Menn, "Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed - sources," May 29, 2015; https://www.reuters.com/article/us-usa-northkorea-stuxnet/exclusive-u-s-tried-stuxnet-style-campaign-against-north-korea-but-failed-sources-idUSKBN0OE2DM20150529.
25. David Sanger and William Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," March 4, 2017; https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.
26. But if the United States is allowed to carry out cyberattacks on Iranian nuclear centrifuges could Pakistan or India use a similar rationale ("he did it first) to attack the other's nuclear supply chain?"
27. For instance, see Ellen Nakashima and Joby Warrick, "For NSA chief, terrorist threat drives passion to 'collect it all'," July 14, 2018; https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.
28. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," February 27, 2019; https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
29. David Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," June 15, 2019; https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.
30. See, for instance, David Sanger, "Russian Hackers Appear to Shift Focus to U.S. Power Grid," July 27, 2018; https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html.
31. David Sanger, Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," February 16, 2016; https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.
32. For instance, see Andy Greenberg, "The Highly Dangerous 'Triton' Hackers have Probed the US Grid," June 14, 2019; https://www.wired.com/story/triton-hackers-scan-us-power-grid/.
33. AFP, "US launched cyber attacks on Iran after drone shootdown: reports," June 22, 2019; https://news.yahoo.com/us-launched-cyber-attacks-iran-drone-shootdown-reports-232123877.html.
34. Not everyone thinks that gaining access against the IRGC (Islamic Revolutionary Guard Corps) would take that long given their state of cybersecurity.
35. "US and Russia clash over power grid 'hack attacks'", June 18, 2019; https://www.bbc.com/news/technology-48675203.
36. Alexandra Ma, "Iran says that US cyberattacks — said to be Trump's preferred retaliation — didn't work," June 24, 2019; https://www.businessinsider.com/iran-us-cyberattacks-after-drone-shot-down-did-not-work-2019-6.
37. For a more elaborated version of that argument, see the author's "Drawing Inferences from Cyber Espionage," Chapter 6 of the T. Minarik et al, 2018 *10th International Conference on Cyber Conflic*t, Tallinn, Estonia (CCDCOE).
38. In other words, the United States would escalate its cyberspace activity for the express purpose of starting a process that yields de-escalation.
39. James Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security*, 43: 1, 56-99.
40. Source: Sumi Somaskanda, "Germany's Cybersecurity Teams Fight 'Ticking Time Bombs'", June 23, 2018; https://www.theatlantic.com/international/archive/2018/06/germany-cyberattacks/561914/.