What if Cyberspace Were for Fighting?

Duncan B. Hollis and Jens David Ohlin

The U.S. military currently regards cyberspace as a warfighting domain,[1] and the United States is one of at least thirty countries building a military capacity to conduct offensive cyberattacks.[2] Of course, the appeal of cyber operations for states is straightforward: they can be deployed to supplement (or even substitute for) traditional means and methods of warfare, such as by disrupting an adversary's command and control networks, military-related critical infrastructure, or weapons capabilities.[3] Further, they can be used asymmetrically, giving otherwise weaker states opportunities to project power. In certain circumstances, they might even operate preemptively as a decisive first-strike capability. At the same time, cyber operations can also contain escalation or provide a consistent means of engagement with adversaries that falls short of kinetic armed conflict.[4]

That said, a few states have expressed anxiety about adopting a "military paradigm" for cyberspace.[5] China and Cuba reportedly refused to endorse the right of self-defense and international humanitarian law (IHL) in cyberspace out of a concern that doing so would legitimize military cyber operations.[6] Given China's own highly regarded cyber forces, its position may be convenient, if not hypocritical, since it is driven by a desire to preserve its room to maneuver and develop its own capabilities, rather than by a sincere concern about the effects that military operations will have on cyberspace.

Whatever the motives of states such as China, the premise—that militarization has significant implications for the future of cyberspace and those who use it—has purchase. As militaries increase their presence in cyberspace, it is important to identify what problems or benefits may result. Moreover, as states and other stakeholders attend to governance both of and in cyberspace, it is important to identify

Ethics & International Affairs, 32, no. 4 (2018), pp. 441–456.

doi:10.1017/S089267941800059X

which legal and policy choices a military paradigm supports. Doing so provides a baseline for comparison with how other cyberspace paradigms (such as those prioritizing economic development or protecting individual freedoms) address the same issues.

In this essay, we explore cyberspace as a militarized domain by envisioning an ideal type—a world that accepts warfighting as *the* prime directive for the construction and use of cyberspace—and examining the ethical consequences that follow. To be clear, we are not arguing that cyberspace is, let alone should become, such a world. But given the range of capabilities that cyber forces provide to states, it is not hard to imagine its appeal in certain quarters. As such, we want to isolate the implications of a warfighting cyber domain as part of the broader effort to understand the reality of a pluralist cyberspace, where ethical imperatives compete or coalesce to support specific governance mechanisms. Doing so may afford greater clarity on which regulatory choices can achieve consensus among competing stakeholder groups as well as on areas where contestation is likely to persist. To this end, we identify below some of the most likely consequences of prioritizing warfighting for (i) who will have authority to regulate cyberspace; (ii) what vehicles they will most likely use to do so; and (iii) what the rules of behavior for states and stakeholders will be. We conclude that states will take on a much greater governance role in such a scenario; and although it is not clear what forms new regulation may take, the content of those regulations will likely preserve and advance state interests (including their interest in conducting warfare) at the expense of information and communication technology (ICT) companies and individuals.

Who Governs in a Warfighting Cyber Domain?

Even if cyberspace exists primarily for war, it does not follow that war would itself become the primary means by which cyberspace would be governed. Unlike land, air, and sea, cyberspace is a sociotechnical institution rather than a natural, physical domain. As Jon Lindsay notes, this means that states must first cooperate in its construction before they can employ it for fighting.[7] This role in constructing and maintaining cyberspace militates against its usage for the most destructive operations (at least compared to kinetic war). As Lindsay writes, the "incentives for moderation are built into its cooperatively constructed infrastructure, and these incentives grow stronger as more economic and administrative functionality moves online."[8] Recent experimental research supports this view.[9] In other

words, as states gain more cyber capabilities, interstate conflicts may become more moderate overall.[10]

At the same time, we do not think a warfighting cyber domain would preserve existing governance structures. Currently, cyberspace has a plurality of governance nodes, including states and multi-stakeholder processes.[11] States regularly exercise jurisdiction over networks and data resident on the hardware located within their territories.[12] Meanwhile, the Internet's domain naming system (as managed by the Internet Corporation for Assigned Names and Numbers, or ICANN) is subject to multi-stakeholder governance, where various communities including—but not limited to—states have a say in its governance. In contrast, such multilateral institutions as the United Nations, the International Telecommunication Union, and the Wassenaar Arrangement have struggled to delineate, let alone operationalize, cyber norms for states to follow.[13]

In a warfighting cyber domain, however, we would expect state-centered, multilateral models to become more prominent. War is a statist concept, and thus multilateral institutions would likely regulate a militarized cyberspace in the same way the United Nations and the Geneva Conventions already do in other use-of-force contexts. Nonstate actors could still play important roles, just as civil society's International Campaign to Ban Landmines was so critical to generating the Ottawa Landmines Convention.[14] But that role is likely to be more a matter of influence and advice than governance per se. In this sense, we would predict ICANN's multi-stakeholder governance structure to flip, elevating the existing Government Advisory Committee (comprised of representatives from 135 state governments) to a more direct regulatory role while de-emphasizing the voices of industry and users more generally. If cyberspace exists for their conflicts, states will want to exercise sufficient control over its architecture and operation.

Whether states can succeed in establishing effective multilateral governance institutions for a warfighting cyber domain is, however, an open question. To be sure, if the "balkanization" of the Internet continues—as more states assert a sovereignty perspective over the ICT environment—we might anticipate formal agreements integrating cyberspace into the Westphalian model.[15] But even then, instead of global governance, we envision like-minded states cooperating in more plurilateral mechanisms. Institutions such as the North Atlantic Treaty Organization or the Shanghai Cooperation Organization might thus have increased importance in a world where warfighting is cyberspace's primary function.

What Forms of Regulation?

Does a warfighting cyber domain suggest particular regulatory forms? Recent debates offer multiple candidates, including treaties, political commitments, customary international law, domestic law, and socialization.

Treaties offer credible expectations of future behavior given the effort and reputational investments involved in achieving agreement, not to mention the completion of domestic legal procedures.[16] But that credibility comes at the cost of time and flexibility, as treaties are notoriously slow to form and equally hard to amend.[17] *Political commitments*, in contrast, are flexible. They generally have no domestic processes for their approval, can accommodate a range of actors beyond states, and more readily allow amendment and exit.[18] However, all of this flexibility tends to make them less credible.[19] *Customary international law* avoids the need for any specific agreement, comprised as it is by a general and uniform state practice accepted as law. But that also creates more room for contestation over both the law's existence and its meaning.[20] Moreover, the capacity for states and others to act anonymously in cyberspace given the technical difficulty of attribution may mean that the most skilled actors' operations go unobserved. This leaves the content of customary law to come from those who cannot anonymize their activity, that is, those who have less experience and skill.[21] *Domestic law* poses no such difficulties and has the benefit of (more) robust enforcement mechanisms. Its difficulty lies in its inability to regulate *interstate* behavior. And when it comes to regulating nonstate actors, domestic law faces issues of dissonance and jurisdiction; different states have different laws, the enforcement of each of which is usually limited to a state's territorial borders. Finally, *cultural or professional norms* may be socialized within a targeted community to ensure particular behavioral patterns. Of course, it should be emphasized that these five candidates are not mutually exclusive; multiple forms may be employed simultaneously or in sequence to regulate a problem.

When it comes to warfighting, treaties would appear to be the gold standard for regulating relations among states. Historically, states have shown a strong preference—via the UN Charter as well as both the Hague and Geneva Conventions—for using treaties to regulate matters of the most serious mutual concern in conflicts.[22] Whether it is the lethality of armed conflicts or the existential threats they pose, states appear to prioritize getting credible commitments to minimize opportunities for participant defections. To date, one of the main obstacles to a

global cyber treaty has been divergent views by states on what cyberspace is "for." Resolving that question in favor of warfighting would give additional support to a global treaty on when or how states may engage in cyberwar.

The preference for treaties with regard to cyberspace, however, may not be universal. Treaties are likely not only where the risk of defection is high and values are aligned but also where actors have sufficient certainty about the object of their regulation. But the ICT environment is, if anything, an arena of innovation, where technology rapidly and dramatically changes in unforeseen ways. Recall, for example, that today's ubiquitous smartphone did not exist a dozen years ago. Therefore, we might expect some caution by states about locking in their warfighting commitments without suitable flexibility for adjustment or exit. As such, it could make more sense for states to sequence their regulatory strategy by beginning not with a treaty but with a more flexible political commitment. A treaty could then follow once states become more comfortable with the arc and speed of ICT capabilities and their ability to control them.

Political commitments could also be a favored method for coordinating how states regulate nonstate actors. Just as the Montreux Declaration clarified obligations and best practices of states with respect to private military and security companies, we could envision similar outcomes in a warfighting-dominant cyber domain.[23]

What about the possibilities of a customary international law for cyber war? Existing efforts to articulate and interpret customary international humanitarian law generally have proved controversial,[24] and such difficulties are exacerbated in cyberspace, given the aforementioned problems of attribution. Even where attribution occurs (for example, U.S. and U.K. accusations that North Korea was behind the WannaCry ransomware[25] or that Russia was responsible for NotPetya[26]), it is notable that no state has situated its complaints in international legal terms.[27] It is difficult to imagine that a warfighting paradigm will resolve such difficulties. As such, we are less sanguine about the possibilities of using customary international law to regulate in this context.

Socialization could, however, play a key role in regulating behavior in our warfighting paradigm. Whatever purchase treaties, political commitments, or domestic law may have, it is often the individuals representing or fighting for states who most regularly demonstrate adherence to the particular norms of their chosen profession. Just as soldiers on the ground (or sailors at sea) behave according to

norms associated with their profession, we expect similar socialization would occur with respect to the regularization of warfighting in cyberspace.

Taken together, just as a warfighting paradigm may privilege certain actors—states—in governing the construction and maintenance of cyberspace, it is also likely to privilege certain regulatory forms. We do not believe any one form will predominate, but we would expect that states and their militaries will seek (and will in large measure succeed) to occupy and regulate cyberspace for military rather than civilian purposes.

What Rules for Behavior?

Adopting a warfighting paradigm might bring about new rules for states, ICT companies, and users, but we expect that the paradigm will depend first and foremost on the law of war as it currently applies to cyberspace. The law of war involves two domains, *jus ad bellum* and *jus in bello*. The former articulates when states can use military force under international law, while the latter regulates the conduct of warfare within an armed conflict. These two legal domains are logically independent, so that both the aggressor state and the victim state (in terms of *jus ad bellum*) are required to follow the same *jus in bello* restrictions. This conceptual independence is the key pillar of the architecture in the legal regulation of warfare.

Although it is unclear how the *jus ad bellum* framework should integrate the possibility of cyberattacks, international lawyers are coalescing around some minimal consensus. Typically, military force is justified only in two situations: (i) when the UN Security Council authorizes a military measure in response to a breach or threat to international peace and security, or (ii) when a state exercises self-defense in response to an actual or imminent armed attack.[28] The self-defense justification only applies in response to an "armed attack," which is a legal concept the precise definition of which has been widely debated. Would a cyberattack constitute an "armed attack" triggering an international right of self-defense that can be executed with kinetic military force? The majority view of the international group of experts who produced the *Tallinn Manual* is that a cyberattack would only constitute an armed attack triggering a right to kinetic self-defense if the cyberattack had real-world consequences that would otherwise meet the standard: for example, the destruction of physical objects such as buildings or the injury or death of humans that meets a minimum scale.[29] What this means is that

cyberattacks that cause widespread disruption to a computer system—but not physical destruction of that system—would not trigger a right of military self-defense.[30]

Of course, just because the cyberattack is not sufficiently destructive to count as an "armed attack" under *jus ad bellum* does not mean that the cyberattack is necessarily lawful, all things considered. The cyberattack might still constitute a violation of other realms of international law, including the duty of nonintervention, the prohibition on violating another state's sovereignty, or (in some limited circumstances) the self-determination of a nation if the cyberattack interferes with a democratic process, such as an election.

The principle of nonintervention itself is well established in international law.[31] The *Tallinn Manual 2.0* states the rule simply: "A state may not intervene, including by cyber means, in the internal or external affairs of another state."[32] As the experts noted, however, "the precise contours and application of the prohibition of intervention are unclear."[33] They emphasized that a cyber intrusion against a foreign state would only count as a violation of the principle of nonintervention if the attack constituted an infringement of another state's reserved domain (or *domaine reservé*) and was coercive in nature.[34] But it is not yet clear what matters are within a state's reserved domain, let alone when a cyber operation would constitute coercion. The increased cyber operations likely to arise in a militarized cyberspace would pressure states to clarify both criteria.

Beyond nonintervention, an even larger debate looms with respect to whether or not state cyber operations against another state can violate a rule of sovereignty. The *Tallinn Manual 2.0* answers that question in the affirmative.[35] Others, however, have questioned whether sovereignty is a stand-alone rule governing state behavior or if, instead, it constitutes a background principle that informs the contents of other rules (such as the duty of nonintervention).[36] Most recently, the U.K. Attorney General placed the United Kingdom in the sovereignty-as-background-principle camp.[37] Nonetheless, in a fully militarized cyber domain, we expect sovereignty to be prioritized such that those favoring sovereignty-as-rule would win out. Still, we expect that the threshold for such a rule's violation will be a high one. Despite some who are inclined to view any cyber intrusion against foreign computer infrastructure as illegal under international law, we think a militarized cyberspace will favor a sovereignty rule targeting only usurpations of an "inherently governmental function," such as the provision of electricity or other essential services, or the administration of elections. This is the prevailing

standard that most (but not all) international lawyers have coalesced around.[38] Currently, states continually engage in low-level cyber intrusions against each other, and the international legal system is unwilling, as of yet, to declare all of them illegal, in large part because states are still experimenting with and developing a better understanding of what exactly cyber operations can achieve. The consequence of such highly restrictive criteria will be to leave room for a substantial amount of cyber "intrusions" that count as statecraft without rising to the level that would be prohibited by international law. At the same time, there would still be a standard for identifying prohibited conduct to make clear that international law has an important role to play in constraining state behavior in the cyber realm.

It is also important to recognize that international law might have other doctrinal routes for regulating cyber activities than the principles of sovereignty and nonintervention. For example, the right of self-determination has bearing on the issue of cyber interference aimed at democratic institutions. Historically, the right of self-determination provided legal grounds for the geopolitical process of decolonization; since then, the concept has waned in significance. But just as the conflicts surrounding decolonization animated concerns for self-determination, we would expect the advent of conflict in a warfighting cyber domain to provoke similar concerns. Some may resist this move because the right of self-determination applies to peoples and nations, rather than states (and international lawyers are uncomfortable with norms that attach to entities other than states). Lawyers may overcome their reluctance, however, because the right of self-determination would provide a powerful argument as to why a cyber intrusion against democratic institutions violates international law. It is not because the cyber activities violate a putative rule of sovereignty, but rather because the activities interfere with the right of a people to use democratic institutions to select their destiny.[39]

Regardless of how the violations are framed, the remedy for these violations might include "retorsions and countermeasures" that take place in the cyber domain.[40] The result might be a tit-for-tat escalation of cyberattacks and responses, each one more serious than the last. The "armed attack" standard will encourage states to fight conflicts below the *jus ad bellum* threshold. These gray zone conflicts will be notoriously difficult to regulate, and our attitude about them will depend on whether they replace, or merely supplement, traditional military conflicts. Subtracting a military conflict and replacing it with a

limited cyber conflict would be a praiseworthy development. On the other hand, simply adding a cyber conflict to an enduring military engagement would expand the warfighting domain to a fourth dimension—hardly a meritorious outcome.

Returning to the law of war as the operating framework, *jus in bello* will involve even more complicated translations of existing laws. Typically, *jus in bello* requires that states limit their attacks to military targets. Civilian collateral damage is only permissible so long as it is not disproportionate to the value of the original military target. Cyberattacks against civilian installations, if they are part of an armed conflict, would therefore violate this core requirement. Furthermore, combatants in an armed conflict are required to wear a uniform, carry their arms openly, and follow the norms of warfare, including the prohibition on perfidy. Cyberattacks launched by a military unit might satisfy this requirement, but if a state uses nonmilitary personnel to carry out a cyberattack that has destructive consequences, the attackers would then be considered unprivileged belligerents subject to enemy capture and punishment—if they can be located at all.

Some states use cyberattacks not just as a force multiplier but also as a form of covert action; they will refuse to acknowledge their involvement and will use personnel connected with a clandestine intelligence agency, who are clearly unprivileged belligerents, to carry out an operation. Of course, some states (including the United States) sometimes refuse to even acknowledge *traditional* military force in situations where acknowledgment would be diplomatically hazardous, such as a drone strike carried out by the CIA, so covert action is certainly not limited to the cyber realm. That being said, we strongly suspect that instances of covert action would increase, rather than decrease, if cyberspace became primarily a warfighting domain.

Rules for States

We predict that states will be subject to an increasing list of overlapping normative constraints, notably international legal restrictions under the law of war, including the rules of *jus ad bellum* and *jus in bello*; and international legal restrictions that apply to gray zone conflicts that fall below the level of intensity typically required for *jus ad bellum* and *jus in bello* rules to apply. At the same time, however, we acknowledge that these regulatory regimes have a shadow side—for every action that is forbidden, others are permitted—which creates a set of de facto licenses that encourage, or channel, state behavior in a new direction. Thus, a militarized cyberspace would continue to preclude states from violating the *jus ad bellum* and

jus in bello criteria, however those thresholds are resolved to respect the novel capacities of ICTs. That said, the laws of war would also inevitably serve to legitimize—and thus empower—states deploying cyber operations that do not run afoul of the law's prohibitions and constraints. The question is whether this shadow licensing is something that should be encouraged or discouraged. We believe that there are strong reasons to encourage some of this licensing, especially when it has the capacity to discourage states from using kinetic attacks that will do far more damage to civilian populations.

Indeed, if cyberspace were truly a zone that existed primarily for states to engage in conflict, it might incentivize such operations or even generate new rules to do so. Today's *jus in bello* rules sometimes produce perverse consequences when applied to cyber operations. Much of the existing *jus in bello* principles, for example, only apply to physical "attacks"—such as the proscription against directly attacking civilians.[41] To date, attacks have been defined in physical terms—operations that generate injuries, death, damage, or destruction.[42] Bombing a factory, for example, constitutes an attack to which the *jus in bello* applies. Assuming that the factory is a lawful military target, the *jus in bello* allows a state to bomb it, causing death and destruction, as long as that attack compares favorably to other attack options, without ever asking if that state could have used cyber means to achieve the same military objective and cause no death or destruction at all. Indeed, it is not clear if shutting down that same factory temporarily via cyber means would even constitute an attack under the legal definition of that term—making it subject to *jus in bello*—if it did not foreseeably generate any death or destruction.

Embracing ICTs as tools for warfare could, however, generate a new rule: a duty to hack.[43] Such a duty would acknowledge the capacity for ICTs to lower the humanitarian costs of war without sacrificing the need to achieve military objectives.[44] It would require that states use cyberattacks in their military operations when they are the least harmful means available for achieving their military objectives. A duty to hack would thus mandate that—all other things being equal—militaries must employ cyber operations when doing so would generate *no* harm versus alternative means and methods that cause *some* harm. Similarly, cyber operations that cause *some* harm must take priority over alternatives that cause *more* harm. In other words, a cyberspace defined by warfighting holds at least some potential to result in less civilian harm than existing kinetic conflicts.

Rules for ICT Companies

The effects of establishing that cyberspace is for fighting would not, however, be limited to regulating interstate behavior. The existing rules for warfare function largely by referencing both the *identity* and *status* of everyone and everything in a conflict: distinguishing state from nonstate actors, lawful from unlawful belligerents, civilian objects from military ones, and so on. As currently constructed, however, cyberspace still has an attribution problem, and this poses obvious challenges for stipulating the identity and status of various actors. To be sure, states and others have shown some recent improvement in their technical capacity (and secondary intelligence) in ascribing responsibility for specific cyber operations. But if cyberspace is primarily for fighting, there will be strong incentives to accelerate existing efforts to ensure proper attribution of cyber behavior. Such efforts might lead to new regulations of state behavior (for example, by requiring a state's military to "mark" its cyber operations or to clearly identify civilian or otherwise protected infrastructure). It seems likely, moreover, that some regulation of ICT companies would follow as well, especially where they produce the hardware and software that constitute the platforms for any cyberattack.

Ideally, ICTs could be the subject of interstate agreements, whether to facilitate attribution directly or assist those identified as its victims. We might anticipate, for example, one or more "duties to assist," requiring participation in some global attribution council, or helping those identified as innocent victims of cyber war.[45] At the same time, we doubt that a warfighting cyber domain would improve attribution in all respects. State militaries, for example, are likely to value encryption technologies to ensure command and control of their own forces, and thus may resist their global regulation. Moreover, efforts by ICT companies to resist cyberspace's militarization (see, for example, the recent "Tech Accords")[46] could become problematic, particularly if such efforts were viewed to favor ICT companies assisting terrorists or otherwise unlawful combatants.[47]

Whatever the prospects for the international regulation of ICTs, we are more confident that a warfighting paradigm would increase efforts to regulate ICTs at the domestic level. If ICTs were primarily a means and method of warfare, states would have a clear interest in controlling their creation and distribution—making them available to allies and denying them to adversaries. In that context, we would expect debates over using terms such as "cyber weapons" to fade, along with the economic, privacy, and research objections that have persisted over using export controls for certain ICTs.[48]

A warfighting paradigm would also incentivize states to approach encryption technologies along two tracks: emphasizing encryption technologies for their own government and military forces, while seeking to minimize their availability for users generally and adversaries specifically. States will have a keen interest in secure ICTs for command and control purposes while also protecting their critical military and civilian infrastructure. Those interests flip, however, with respect to foreign and commercial ICTs where a state's interest would most likely favor access to the source code and contents thereof, especially if this would provide enhanced visibility as to who might attack them or how they might do so. Whatever privacy concerns might govern in peacetime, such interests in access may even extend to requiring ICT companies to offer the state limited access to their systems, whether for threat monitoring or as leverage for external offensive operations.

Rules for Users

Similar motivations could lead states to impose regulations on all users. As noted, states on a war footing are more likely to expect users to sacrifice their privacy or economic interests in favor of national security. Each state is likely to have an interest in data localization rather than the generative and innovative aspects of a more global network.[49] A national cyber infrastructure is easier to monitor, defend, control, and deploy in a conflict than a global system. Data localization could, for example, enable states to better protect against insider threats and provide additional avenues to surveil and monitor for malware implants by foreign actors in domestic systems and networks. Thus, we expect the warfighting domain would further divide ICT usage along national lines.

Would prioritizing national security over the rights of individual users resolve existing debates over hacking back? These debates center on the question of whether domestic laws should allow individual victims of cyberattacks to pursue their attackers. Currently, ethical claims in support of hacking back rest on various grounds, including individual rights of self-defense, economic interests in protecting intellectual property, and public health analogies aspiring to "clean up" the system.[50] Prioritizing these claims would certainly advance the case for hacking back.

But if the prime directive is to retain cyberspace for warfighting, states are likely to deny individual users any justifications for behavior that could interfere in a state's ability to control conflicts. In such circumstances, hacking back is most

likely to be viewed either as a threat to the rule of law or as a risk of starting or escalating armed conflict. To be sure, some argue that these risks are overstated, claiming that at most hacking back equates to a "frontier incident" that cannot justify a state's use of force.[51] Moreover, depending on their capabilities, states are likely to employ private actor proxies—whether civilian "militias," organized groups, or individuals—to fight on their behalf, which would amount to a tacit approval of hacking back.[52] But neither of these rationales supports true vigilante behavior. On balance, therefore, we believe states will exercise caution in authorizing—and are more likely to oppose—users hacking back outside state control.

Conclusion

Many cybersecurity and cyber policy debates today elicit dramatically different—and competing—regulatory proposals. One reason for such disagreement lies in different visions of what cyberspace is "for." Although we take no position whether cyberspace should (or should not) be a domain where warfighting is the prime directive, it seems clear that such a vision would have significant consequences for who would govern, how they would do so, and what the rules would be.

What would a cyberspace for fighting look like? We believe it is one where states would take on a greater (but not exclusive) role in governing all aspects of the technical architecture and infrastructure. States are likely to do so through treaties or political commitments at the international level, with domestic laws and socialization efforts playing out in other contexts. It will not, however, be a world without law. On the contrary, we would expect the concepts of *jus ad bellum* and *jus in bello* to take on greater importance as states use them to gauge their cyber operations. Moreover, states may fall back on a set of secondary rules (nonintervention, sovereignty, self-determination) to guide their cyber operations when they remain below the threshold for armed conflict. We expect that in doing so, states might actually end up causing less harm (whether through a duty to hack or a more general commitment to preserving cyberspace as a sociotechnical institution) in interstate conflicts. While this might be a positive outcome for civilians, the downside for them is that they might be regulated more, whether in terms of ICTs being told how to deal with encryption or individual users being limited in their capacity to hack back in self-defense. Whether or not cyberspace evolves along these lines is, of course, an open question.

NOTES

[1] *Summary of 2018 National Defense Strategy of the United States of America* (Washington, D.C.: U.S. Department of Defense, 2018), p. 6. The United States began to regard cyberspace as an operational domain in 2011. *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: U.S. Department of Defense, 2011), p. 5; and David Alexander, "Pentagon to Treat Cyberspace as an 'Operational Domain,'" *Reuters*, July 14, 2011.

[2] Steve Ranger, "US Intelligence: 30 Countries Building Cyber Attack Capabilities," *ZDNet*, January 5, 2017.

[3] See, for example, *The Department of Defense Cyber Strategy* (Washington, D.C.: U.S. Department of Defense, 2015), p. 14.

[4] U.S. Cyber Command, for example, has recently emphasized the latter capacities in delineating its strategies for future operations. See, for example, Richard J. Harknett, "United States Cyber Command's New Vision: What It Entails and Why It Matters," *Lawfare*, March 23, 2018.

[5] Zhixiong Huang and Kubo Mačák, "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches," *Chinese Journal of International Law* 16, no. 2 (2017), p. 299 (quoting Ma Xinmin, a senior Chinese diplomat and international lawyer).

[6] See, for example, Julian Ku, "How China's Views on the Law of *Jus Ad Bellum* Will Shape Its Legal Approach to Cyberwarfare," Aegis Series Paper No. 1707, Stanford University, Hoover Institution (2017), p. 2; and Arun M. Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare*, July 4, 2017.

[7] Jon Randall Lindsay, "Restrained by Design: The Political Economy of Cybersecurity," *Digital Policy, Regulation and Governance* 19, no. 6 (2017), p. 493.

[8] Ibid., p. 494.

[9] Benjamin Jensen and David Banks, "Cyber Operations in Conflict: Lessons from Analytic Wargames," UC Berkeley, Center for Long-Term Cybersecurity Occasional White Paper Series (2018), cltc.berkeley.edu/wp-content/uploads/2018/04/Cyber_Operations_In_Conflict.pdf.

[10] Ibid., p. 3.

[11] See Laura DeNardis, *The Global War for Internet Governance* (New Haven, Conn.: Yale University Press, 2014), ch. 1.

[12] Jack L. Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006); and Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64, no. 3 (2015), p. 677.

[13] See, for example, Arun M. Sukumar, "The UN GGE Failed"; Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," *Lawfare*, January 5, 2018; and Vinton Cerf, Patrick Ryan, and Max Senges, "Internet Governance Is Our Shared Responsibility," *I/S: A Journal of Law and Policy for the Information Society* 10, no. 1 (2014), pp. 1–42.

[14] See Richard Price, "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines," *International Organization* 52, no. 3 (1998), p. 613.

[15] See Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (2011), pp. 32–61 (predicting states will delineate cyberspace "by formal agreement" with a "new cyber–Westphalian process" and "digital regions complete with borders, boundaries, and frontiers that are accepted by all states").

[16] Duncan B. Hollis and Joshua M. Newcomer, "'Political' Commitments and the Constitution," *Virginia Journal of International Law* 49, no. 3 (2009), p. 507; Kal Raustiala, "Form and Substance in International Agreements," *American Journal of International Law* 99, no. 3 (2005), p. 581; and Charles Lipson, "Why Are Some International Agreements Informal?" *International Organization* 45, no. 4 (1991), p. 495.

[17] Some modern treaties (such as multilateral environmental agreements) attempt to overcome this problem by devising built-in adjustment mechanisms to accommodate new facts, scientific developments, or agreements. Jutta Brunneé, "Treaty Amendments," in Duncan B. Hollis, ed., *The Oxford Guide to Treaties* (Oxford: Oxford University Press, 2012), p. 347; and Laurence R. Helfer, "Nonconsensual International Lawmaking," *University of Illinois Law Review* 1 (2008), p. 75.

[18] Hollis and Newcomer, "'Political' Commitments and the Constitution," pp. 512, 526.

[19] Raustiala, "Form and Substance in International Agreements," p. 613; and Lipson, "Why Are Some International Agreements Informal?" p. 511.

[20] See Duncan B. Hollis, "The Existential Function of Interpretation in International Law," in Andrea Bianchi, Daniel Peat, and Matthew Windsor, eds., *Interpretation in International Law* (New York: Oxford University Press, 2015), p. 78.

[21] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110 (2016), p. 471.
[22] See, for example, UN Charter, Ch. VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression; Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, August 12, 1949, UNTS 75, p. 287; and Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, October 18, 1907.
[23] "The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict," Government of Switzerland and the International Committee of the Red Cross (2008). For a proposal along these lines, see Wyatt Hoffman and Ariel (Eli) Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* (Washington, D.C.: Carnegie Endowment for International Peace, 2017).
[24] Compare Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, International Committee of the Red Cross (New York: Cambridge University Press, 2005) with "Letter from John B. Bellinger III, Legal Adviser, U.S. Department of State, and William J. Haynes, General Counsel, U.S. Department of Defense, to Dr. Jakob Kellenberger, President, International Committee of the Red Cross, Regarding Customary International Law Study," November 3, 2006, reprinted in *International Legal Materials* 46, no. 3 (2007), pp. 514–15.
[25] Nate Lanxon and Tim Ross, "U.K. Blames North Korea for WannaCry Attack on Health Service," *Bloomberg*, October 26, 2017; and Dustin Volz, "U.S. Blames North Korea for 'WannaCry' Cyber Attack," *Reuters*, December 18, 2017.
[26] Sarah Marsh, "US Joins UK in Blaming Russia for NotPetya Cyber-Attack," *Guardian*, February 15, 2018.
[27] See, for example, Kristen Eichensehr, "Three Questions on the WannaCry Attribution to North Korea," *Just Security*, December 20, 2017; and David P. Fidler, "Was Stuxnet an Act of War? Decoding a Cyberattack," *IEEE Security & Privacy* 9, no. 4 (2011), p. 56 ("Nation-states have been curiously quiet about Stuxnet…including the victim state (Iran)"). With respect to the Sony Pictures hack, President Obama declined to classify the incident as cyber warfare but referred to it as an act of "cyber vandalism." Brian Fung, "Obama Called the Sony Hack an Act of 'Cyber Vandalism.' He's Right," *Washington Post*, December 22, 2014.
[28] See UN Charter, Articles 39, 42, and 51.
[29] See Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), Rule 71 ("A state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense.").
[30] Ibid. (referring to "scale and effects" of the attack).
[31] See, for example, UN General Assembly Resolution 2625 (XXV), "Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States," October 23, 1970, A/RES/25/2625; and Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States), ICJ Reports 1986, p. 97–98 [para. 205]; see also Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, ICJ Reports 2005, p. 63 [para.163].
[32] Schmitt, *Tallinn 2.0*, p. 312.
[33] Ibid., p. 314.
[34] For a discussion, see Gary P. Corn and Robert Taylor, "Sovereignty in the Age of Cyber," *AJIL Unbound* 111 (2017), pp. 207–12.
[35] Schmitt, *Tallinn 2.0*, p. 17 (Rule 4).
[36] See, for example, Gary Corn, "Tallinn Manual 2.0—Advancing the Conversation," *Just Security*, February 15, 2017.
[37] Jeremy Wright, QC, MP, "Cyber and International Law in the 21st Century," May 23, 2018, www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
[38] Schmitt, *Tallinn 2.0*, pp. 21–24.
[39] See Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95 (2017), pp. 1579–598.
[40] On retorsions and countermeasures, see International Law Commission, "Draft Articles on the Responsibility of States for Internationally Wrongful Acts," in *Report of the International Law Commission on the Work of its Fifty-Third Session*, UN Doc. A/56/10, pp. 128–37 (articles 49–53).
[41] See the Protocol Additional to the Geneva Conventions of August 12, 1949, and relating to the Protection of Victims of Armed Conflicts (Protocol I), June 8, 1977, UNTS 1125, p. 3, articles 48 (regarding distinction), 57(2)(a)(ii) (regarding precautions).

[42] See Schmitt, *Tallinn 2.0*, pp. 415–22 (Rule 92).
[43] One of us has written about such a duty in some detail. See Duncan B. Hollis, "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack," in Jens David Ohlin, Kevin Govern, and Claire Finkelstein, eds., *Cyberwar: Law and Ethics for Virtual Conflicts* (New York: Oxford University Press, 2015), p. 129.
[44] Michael Schmitt, "Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance," *Virginia Journal of International Law* 50, no. 4 (2010), p. 795.
[45] See, for example, John S. Davis II et al., *Stateless Attribution: Toward International Accountability in Cyberspace* (Santa Monica, Calif.: RAND Corporation, 2017).
[46] See David E. Sanger, "Tech Firms Sign 'Digital Geneva Accord' Not to Aid Governments in Cyberwar," *New York Times*, April 17, 2018.
[47] See, for example, Charlie Dunlap, "Why Companies Should Not Sign the 'Cybersecurity Tech Accord,'" *Lawfire*, April 21, 2018.
[48] See, for example, the Wassenaar Arrangement, www.wassenaar.org (detailing export controls participants should adopt domestically for certain intrusion software and IP network surveillance systems).
[49] See generally Chander and Lê, "Data Nationalism."
[50] See, for example, Stewart Baker, Orin Kerr, and Eugene Volokh, "The Hackback Debate," *Steptoe Cyberblog*, November 2, 2012, www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.
[51] Patrick Lin, "Ethics of Hacking Back—Six Arguments from Armed Conflict to Zombies," U.S. National Science Foundation Paper, Sept. 26, 2016.
[52] See generally Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018).

Abstract: This essay explores the ethical and legal implications of prioritizing the militarization of cyberspace as part of a roundtable on "Competing Visions for Cyberspace." Our essay uses an ideal type—a world that accepts warfighting as the prime directive for the construction and use of cyberspace—and examines the ethical and legal consequences that follow for (i) who will have authority to regulate cyberspace; (ii) what vehicles they will most likely use to do so; and (iii) what the rules of behavior for states and stakeholders will be. We envision a world where states would take on a greater role in governance but remain constrained by law, including *jus ad bellum* and *jus in bello* criteria, but also sovereignty, nonintervention, and self-determination. We ask if the net result would mean states causing less harm than they do in kinetic conflicts. Ultimately, our essay takes no position on whether cyberspace should be a militarized domain (let alone one where warfighting is the prime directive). Rather, our goal is to situate a warfighting cyber domain within the reality of a pluralist cyberspace, where ethical imperatives compete or coalesce to support specific governance mechanisms.

Keywords: cyber war, cyberspace, cyberattack, *jus ad bellum*, *jus in bello*, international humanitarian law, global governance, hacking back