COLUMBIA | SIPA
School of International and Public Affairs

CCSA
Cyber Conflict Studies Association

The International Law of Cyber Conflict

AUTHOR AND SERIES EDITOR: Justin Key Canfil
EXECUTIVE EDITOR: Jason Healey

Introduction

Is there international law to govern cyberspace and/or cyberspace operations? For years, this has been the million-dollar question. There is growing consensus that, far from the "wild west" it is often depicted as, cyberspace is indeed subject to extant legal and normative regimes. However, agreement on precisely which rules apply has proven elusive, and important issues remain unsettled. Participants in the 2017 State of the Field (SOTF) conference explored these issues through three main questions: (1) has progress been made in recent international legal discourse or diplomacy?; (2) does proposed theory reflect the reality of state practice?; and (3) what are the most important emerging issues?

The 2017 SOTF conference builds on findings from the 2016 SOTF conference, as well as several subsequent real-world developments. It first engages in a brief review of the findings of the 2016 panel. Next, it examines whether any theoretical progress has been made in the intervening period. It then turns to the question of whether theory accords with observed state practice. The years 2015 through 2017 saw numerous attempts by the international community to iron out consensus on the most pressing cyber law issues, but how closely do the fruits of these efforts mirror the claims of theorists and advocates? Finally, the report concludes by calling attention to several critical emerging issues and recommendations for future research areas.

About the State of the Field Series

This article is part of the 2017 Cyber Conflict State of the Field (SOTF) paper series, under the auspices of the Cyber Conflict Studies Association and Columbia University's School of International and Public Affairs.

The conference, held annually since 2016, brings together experts from various academic disciplines, including political science, law, economics, and policy research, to define key questions and map the research frontier in the emerging field of cyber conflict studies. The conference is cumulative: each year builds upon past discussions. As a result, discussions have necessarily matured at different rates as new topics are added.

The papers in this series are meant to capture the findings of the 2017 conference. Together, the papers represent the conference attendees' understanding of the present state of the field in the academic study of cyber conflict.

2016 Review

The 2016 SOTF Law and Ethics discussion broached three topics: *jus ad bellum*, the law governing the rights of states to resort to uses of force; *jus in bello*, the law that governs within armed conflict; and general issues involving sovereignty and neutrality. Leaning heavily on the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, the 2016 working group's core premise was that, although legal ambiguity and challenges in enforcement remain, there has been a general trend towards consensus that international law does

govern cyber operations, and on the application of some specific, fundamental principles of international law to the cyber domain. Lawyers and other interested stakeholders have undertaken the task of interpreting precedent [. . .]"in the hope that presenting a coherent legal framework will encourage states to embrace certain norms."[1,2] It is from that premise that this report proceeds, by examining more recent developments for evidence that international opinion is converging on a particular set of solutions.

The most important function of the 2016 report was to serve as a compilation of a body of canonical literature on the topic of cyber law. As the text notes, "rarely is a single author, work, or school of thought the starting point for a legal analysis in the manner that those might be in, for example, the field of international relations."[3] The usual canonical sources in international jurisprudence—treaty law, customary international law, and reference points such as landmark International Court of Justice (ICJ) precedent—largely arose before the advent of the cyber domain. Thus, given the proposition that extant legal regimes apply to cyberspace, panelists at the 2016 conference rightly recognized that importing such sources from across domains threatened to inject the discussion with an implicit tautology. Instead, "canonical" was taken to mean "works that have made a *direct* contribution to the relatively young field of the law governing cyber conflict. With a few notable exceptions, most are scholarly works," such as the *Tallinn Manual* and earlier writings.[4] The group saw the *Tallinn Manual*'s findings as *de rigeur*, especially on issues of *jus ad bellum*. However, several unanswered questions remained at the time of drafting:

- On cyber conflict below the threshold of *jus ad bellum*: how can retorsion and countermeasures be meaningfully distinguished? Which legal framework is ideal for sub-threshold incidents?
- On *jus in bello*: although international humanitarian law precepts apply, what can be done if states reject their application to cyber incidents? Note that this is a problem across operational domains, heightened by cyberspace characteristics. What types of persons or infrastructure qualify for protected status? How should cyber infrastructure be classified or distinguished?
- On sovereignty and neutrality: when does a third-party state forfeit neutrality? For the conduct of non-state actors, which test—effective versus overall control—is more sensible? What responsibility does the state have for the private sector?

On these and other questions, the 2016 SOTF workshop looked forward to further exploration in the relatively young body of scholarship dedicated to cyber law. However, participants cautioned that "those working on cyber conflict should approach the law with an appreciation for its inherent uncertainty. The emergent field of cyber conflict law is highly dependent on interpretation and implementation. Each new international cyber incident presents the potential for upending existing assumptions."[5] It was with that caveat in mind that the 2017 workshop participants sought to examine progress, developments in the relationship between theory and practice, and key emerging issues.

2017 Takeaways

The law and ethics panel arrived at several conclusions and broached several topics for which answers are not yet clear. This particular constellation of participants reminded the group of the utility of thinking about law in "two separate buckets": domestic and international. Thus far, cyber conflict discussions both in the literature and at SOTF Conferences have primarily concerned themselves with questions of public international law. Domestic law, especially the Title 10/ Title 50 debate concerning the blended role of military and intelligence operators in cyberspace under U.S. federal law, has often been overlooked by scholars.

Participants also discussed whether the "use of force" debate in the legal literature, which seeks to apply *jus ad bellum* concepts to cyber operations, is the most fruitful avenue for discourse. Several participants complained that, although the issue has been debated for over 20 years, all scholars have succeeded in doing is to clarify the questions. Furthermore, participants insisted that some operations will never fit into the use of force construct. Given this limitation, participants considered alternate paradigms for regulating operations below the "armed attack" threshold that triggers a state's inherent right to self-defense, including environmental law, public health law, and other *lex specialis* models that

might make suitable analogs. They also considered whether sovereign noninterference might be a superior way to frame the issue.

Until states act, theories remain abstract. To solve many cyber problems, the world needs to build norms. However, as working group participants highlighted, many cyber characteristics—such as being clandestine and multi-stakeholder—heighten the challenges of norm development. Also at issue is the question of who gets a seat at the table. A greater number of seats would mean more buy-in from the international community, but at the cost of impeding consensus and diffusing control over outcomes. Beyond the number of seats is the question of who should populate those seats. Norms resultant from any working group directly reflect the interests of those shaping the norms. For example, if the great cyber power shape the norms, it is like those norms will best support the interests of the great powers at the costs or tertiary cyber actors.

The working group also tackled the important task of clarifying terms and definitions, specifically for the concepts of "norms" and "operations" in cyberspace. This exercise revealed a high degree of heterogeneity in the thinking of even a relatively homogenous (mostly American) group. Perhaps the most important outcome was the reiteration that norms are what states do, not what they expect. Not every offense is a "violation." The group then had a deeper debate over who it spoke for: Global citizens? International legal scholars? The United States? The working group alone? The group members as individuals? As this discussion made apparent, participants all wore different hats, which were difficult to remove, complicating their task of elucidating the state of the cyber conflict field.

Finally, the group tried to answer the question of whether cyber norms can only emerge through catastrophe. Although views were mixed, they were primarily optimistic: even if idealism does not carry the day, the threat of catastrophe can motivate just as well as catastrophe itself. States have managed to forecast and regulate (if not solve) many problems before they resulted in tragedy. Examples of successful precautionary regulation include treaties governing nuclear proliferation and space. It should be noted, however, that the 2017 SOTF conference was held not long before the United Nations Group of Governmental Experts (GGE) meeting, which ended the previously positive trend in cyber norm development by failing to reach consensus.[6] In any case, it cannot be known what the future holds.[7] Whether or not a catastrophe is necessary to catalyze norm formation, is one likely to occur?[8] The novelty of cyber means is commonly thought to raise the risk of inadvertent or accidental escalation, but we might also expect states' mutual interest in stability to be a dampening force. Furthermore, ambiguity in states' beliefs (and beliefs about their adversaries' beliefs) about cyber law may actually help in some cases by dampening enthusiasm for potentially provocative attacks.

Filling the Gaps: Recent Theoretical Progress

After defining terms for the purpose of the discussion, workshop participants addressed select "gaps" identified in the 2016 report: (1) the regulation of low-level conflict; (2) appropriate thresholds and standards for (a) the activation of the right to national self-defense, and (b) attribution of state responsibility for acts by non-state actors; (3) problems related to overlapping jurisdictional claims and enforcement; and (4) remaining controversies in international humanitarian law. Finally, they asked how definite markers for international norms and *opinio juris* (the beleive that an action is taken out of a sense of legal obligation) can be recognized in practice.

Definitions

The group recognized that while new definitions cannot entirely quell internal disagreement over policy preferences, cogent terminology helps prevent talking at cross purposes. Therefore, the participants' first task was to converge on definitions for several key terms, including "cyber operations" and "norms." The U.S. Army describes "cyber operations" as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives . . . or to intimidate any person in furtherance of such objectives."[9] Matthew Waxman puts it more succinctly: "Efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them."[10] Participants criticized these definitions as too focused on comput-

ers and computing systems, overlooking the personnel behind the keyboard as well as the Internet of Things (IoT)—assets beyond the digital. They also experienced difficulty in pinning down "evolving" technical terms, such as "network." Finally, conventional definitions of "operations" were seen as concentrated too much on attack and offense.

The definitions given to "Norms" in the social science literature range from "standards of appropriate behavior for actors of a given identity," to a special class of social institutions (or what Douglas North calls "rules of the game . . . [or] humanly devised constraints").[11] Participants considered whether "acceptable" should be substituted for "appropriate," reasoning that norms only become norms when they are diffused, which requires acceptance from other actors. One participant advised that "norms" be defined as both acceptable and *expected*, since many actions may be "acceptable" but never done and thus are not "normal" behavior. Finally, participants agreed that norms are what actors *do*, not what they *want*. For example, it is not a *violation* of any established norm to "dox" politicians, merely an affront. This distinction is important; if the positions held by cyber law advocates fail to reflect state practice in the international system, then their tenets are merely aspirations rather than decided norms.

Self-Defense Thresholds

Participants agreed that *jus ad bellum* customary law governs the permissibility of operations exceeding the threshold of "armed attack" articulated by the ICJ.[12] However, two problems remain. First, where is that threshold in practice? How would we know when a cyber operation had exceeded it? The answer is important both for preventing serious attacks (if a line is drawn, attackers might be deterred from crossing it) and for remedying serious attacks if and when they occur (dispute settlement fora need standards on which to draw, and the international community may need to be persuaded that the line has in fact been crossed). Yet, as participants noted, this question has already been debated for decades with no convincing answers. One participant described the obsession with this question as a "suffocating legal asymmetry," arguing that the United States is "paranoid" about committing an act of war, failing to recognize that, due to the extreme power imbalance between the United States and other states, very few (if any) U.S. actions in cyberspace, no matter how catastrophic or insidious, would be construed by its adversaries as *casus belli*. Whether or not this type of risk aversion is pervasive, it is counterintuitive to international relations theories about escalation in gray zones.

Not all cyber news is bad news. Since the 2016 SOTF report, theories on self-defense and state responsibility have advanced significantly, thanks in large part to the release of the *Tallinn Manual 2.0*. The *Tallinn Manual 1.0* outlined only basic thought on the circumstances in which retorsion or other countermeasures, often the only legal recourse a victim state has against a perpetrating state, might be permissible. The second *Manual* builds on the first to offer more specific advice, particularly with respect to cross-domain countermeasures. It also clarifies where the boundaries of knowledge lie: the *Manual*'s authors could not agree on whether collective security countermeasures were permissible, and no provision for countermeasures against non-state targets could be made (although the authors did agree that the "plea of necessity" for actions against non-state actors was reasonably analogous between cyber and conventional domains).

State Responsibility

For non-state actors to be held accountable, their actions must be connected to a state. As the UN General Assembly and UN GGE articulated in 2013, the principle of sovereignty, and thus the state veil protecting malicious non-state actors from international accountability, continues to hold in cyberspace. However, the UN Charter's exhortation for peace and security also applies, illustrating an inherent tension in public international law. Fortunately, the missing link—the law of state responsibility—has been slightly clarified since the 2016 SOTF report. The bad news is that this body of law does little to disincentivize state delegation to non-state actors, i.e., proxy wars, particularly in the cyber domain, where attribution to the state may be difficult to prove. The *Tallinn Manual 2.0* explains that extant state responsibility law applies, but not in a one-to-one mapping because virtual military assets, unlike physical ones, can be easily spoofed or commandeered. Given this difference, a more restrictive test of state "control" might be required. Similarly,

although financial aid to malicious non-state groups is discouraged, state patrons are responsible only for the provision of aid itself, not for what non-state actors do with it. In the context of cyber conflict, the provision of aid—in the form of knowledge, funding, or code—may be all that is required for a non-state group to carry out complex and wide-ranging operations.

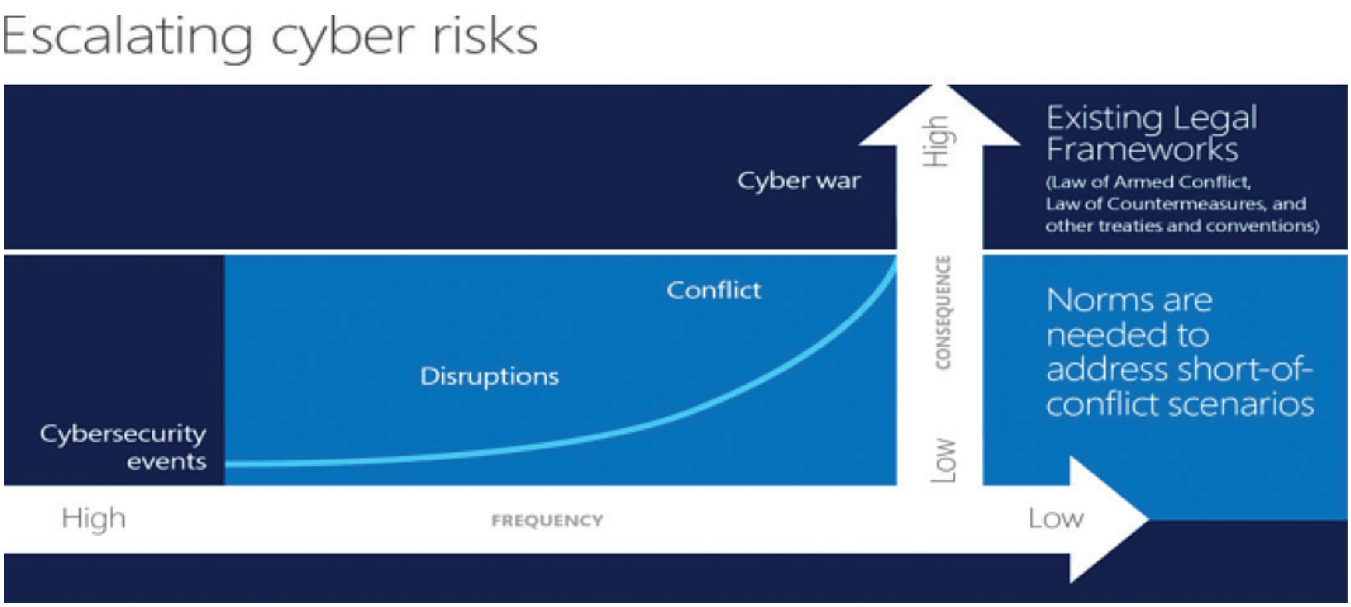
Other scholars have examined this issue. For example, a "Symposium on Cyber Proxies" was held at Columbia's School of International and Public Affairs in the spring of 2016.[13] Others have stressed the need to search outside of conventional sources of state responsibility law[14] for helpful general principles, including *sic utere tuo ut alienum non laedas* (use your own property so as not to harm another), which may also apply.[15] As Katharina Ziolkowski argues, the fact that states do not advertise their delegation to proxies gives weight to the idea that *opinio juris* may already exist in a liminal state.[16]

Even when state responsibility law is clear, operationalizing it requires technical attribution that is sometimes beyond the victims' capability.[17] While the international community may know victimization when it sees it, is case-by-case consideration enough, or must a clear legal standard for the burden of proof be developed? More efforts are needed to bridge applied legal standards with technical standards.[18] Participants agreed that another complication—and potential solution—lies in the increasing importance of private cyber intelligence firms, which are not subject to the same political or reputational constraints as governments or corporate data holders. The empirical question of whether the rise of private cyber intelligence firms has actually enhanced states' ability to hold perpetrators accountable remains unanswered. The proliferation of national disclosure laws and international Computer Emergency Readiness Team (CERT) cooperative arrangements may further support efforts to boost transparency.

Paradigms for Low-Level Operations (LLO)

Self-defense against armed attacks, a relatively easy debate, may not be the most necessary one. Much more difficult is the debate over how to regulate operations that definitely fall below the threshold of an armed attack or even a use of force. Angela McKay of Microsoft has stressed that whereas international law governs the region above the threshold, norms are needed to address everything else.[19] Figure 1, courtesy of Microsoft, illustrates this threshold.[20] Participants concurred that Figure 1 accurately represents the current framework and that the UN Charter Article 51 (referring to the right to self-defense) line could only be crossed by a cyberattack of extraordinary scale. However, participants (and, more broadly, scholars and states) have not reached consensus about the precise location of that line. Participants also noted a lack of evidence of any concrete norms in the sub-Article 51 region.

FIGURE 1: Use of Force Framework



Rather than continuing to debate the location of the armed attack threshold, some panelists urged that the issue be reframed in terms of sovereignty. While LLOs will likely never be regulated by self-defense principles, they might be governed by the principle of sovereign non-interference.[21] Ironically, sovereignty—or rather, the normative prohibition against sovereign intrusions in international relations—is the way states such as China and Russia have traditionally framed the cyber debate. Although Western countries view the Internet fundamentally differently, as a domain that inherently transcends national borders, this is one area where a mutually agreeable bargaining solution may exist, potentially opening up space for new norms.

Of course, as some participants pointed out, the United States seems relatively accepting of inward-facing sovereignty standards (such as China's "Great Firewall") while less accepting of transborder activities (such as the 2015 attack on Github, for which China was blamed).[22] Likewise, the whole of the working group acknowledged practical limitations of applying sovereign non-interference to cyber activity. Establishing a shared definition of "sovereignty" in cyberspace, a necessary first step, would trigger fierce disagreement among states. While a well-established set of extant law on sovereignty could be ported, the political feasibility of states adhering to that law remains dubious.

Also at issue is the controversy over which existing legal paradigm might offer the greatest traction over LLOs. The concept of the "use of force" applies below the threshold of "armed attack" in theory, but its precise application is subject to considerable debate. Moreover, even if it were possible to establish an action as "unlawful" because it constituted a use of force in cyberspace, enforcement would present significant challenges in practice. The working group explored three alternative models. First, the criminal model espoused by one school of scholarly thought argues that direct culpability lies with individual perpetrators. When such individuals act of their own accord, frameworks like the Budapest Convention[23] and a system of overlapping mutual legal assistance treaties (MLATs) provide the means for victim states to seek justice.[24] But this paradigm falls short when LLOs are conducted on behalf of a state. Additionally, the system of MLATs and criminal cyber conventions is incomplete. The Budapest Convention, while a significant milestone, is not comprehensive and has not been ratified by many states. Further, many states lack bilateral MLATs with one another. Conflicting jurisdictional claims are another potential problem.

Participants next considered the environmental model.[25] Customary environmental law is based on doctrines such as the "no harm" and "good neighborliness" principles, which have been reaffirmed in several ICJ cases.[26] While transborder toxic spills, harmful emissions, and water contamination make colorful analogies, however, this body of law is largely undeveloped. There is a dearth of primary sources such as robust customary rules. Treaties drafted strictly for environmental issues would have to be renegotiated for cyber operations *per se*. Environmental law is also intensely fact-based, making it a poor analog for cyberattack victims with limited forensic capabilities or disincentives to public disclosure.

Finally, participants considered the possibility that no extant model adequately fits. The scenario in which these LLOs are *non liquet*, as the earliest cyber legal theorists argued, presents both the greatest opportunity and greatest risk.[27] A new, well-designed, universal treaty would theoretically allow the international community to tailor legal standards to cyber operations. However, the divisiveness of the issue and political self-interest of states call into question the feasibility of *lex feranda*.[28] The rapporteur notes that this approach could also be a double-edged sword in that, until a cyber treaty is negotiated, treating cyber LLOs as *de novo* is an admission that the zone below armed attack is indeed the "wild west."

Participants also considered possible models not yet proposed in the literature, including public health, cross-sectoral retaliation (an economic concept), and the common/maritime law principle of hot pursuit, which allows for the pursuit of suspected belligerents across ordinary jurisdictional boundaries under exigent circumstances. Another proposal was to apply the "unwilling and unable" doctrine to cyberspace, although it is not clear how the doctrine, which is highly contested when applied to traditional military interventions, fits with LLOs, which are, by their nature, limited.[29] Counterintuitively, another possibility is to simply take a more permissive view of the law on countermeasures in the hopes that mutual risk will encourage host states to crack down on low-level activity.[30]

Jurisdiction & Enforcement

"Jurisdiction" refers to "the competence of States to regulate persons, objects, and conduct under their national law, within the limits imposed by international law."[31] In international law, jurisdiction is usually divided into three categories: prescriptive, adjudicative, and enforcement. Discussions around cyber law usually relate to the first category—the creation or articulation of rules in cyberspace. Scholarly attention has increasingly turned to the latter two; that is, the rights of states to respond when these rules are broken. Unfortunately, findings have only elucidated how limited these rights actually are.

"Jurisdiction to adjudicate," in this case, refers to the right of states to subject persons suspected of perpetrating cybercrimes to trial in courts with competency to hear such cases. As with physical claims, the strength of this type of jurisdiction turns on physical territoriality: extraterritorial jurisdiction over cybercrimes must be based on conventional principles.[32,33]

The legal concept of "jurisdiction to enforce" refers to the right to intervene against cybercrimes emanating across national borders. Extending this type of jurisdiction is an inherently political problem. The paucity of avenues for addressing cybercrime intensifies existing challenges. Enforcement against malicious actors who operate across borders hinges on the cooperation of host states. When host states are uncooperative, accusers generally have few legal avenues to resolve their grievances. Greater encouragement of MLATs or treaty frameworks like the Budapest Convention might help address this lack of recourse. Since there has been little scholarly work on MLATs since 2016, this may constitute a research opportunity. Others scholars have raised the idea of erecting an international cybercrime court to which states could submit their claims.[34] Short of that, coercive instruments, such as economic sanctions, may be the only means of resolution available to states that feel they have been wronged.

Controversies in International Humanitarian Law (IHL)

The debate over IHL's application to cyber warfare historically ranged between three schools. Idealists argued that, despite the fact that nowhere is cyber specifically enumerated in the law of armed conflict, non-derogable rules organically emerge by analogy or through public conscience.[35] Realists, conversely, postulated that applications exist but are more limited; namely, only beyond the kinetic divide.[36] Finally, skeptics held that IHL applies strictly to conventional domains, that cyber is *sui generis*, or that the factual challenges are insurmountable.[37]

As of 2017 and the publication of two *Tallinn Manuals*, this debate has (in theory) been settled. IHL applies in a restrictive sense, somewhere between the idealist and realist positions. The second *Tallinn Manual* further clarifies Geneva, consular, and human rights law, for instance by holding that the personally identifiable information of *hors de combat* and diplomatic staff are protected in times of war.[38] Still unanswered are several other important questions, such as clarifying what core IHL principles—including the prohibition on acts of perfidy and rules requiring fixation of distinctive emblems—would look like in cyber operations.

Theory Versus Reality: Developments in Practice

Linking theory and practice requires a quantitative analysis of state behavior and beliefs (*opinio juris*), the two necessary criteria for determining the emergence and formation of customary international law. While state practice on larger cyber issues, such as self-defense and IHL, has been limited, there is a growing body of data tracking unilateral state expressions. This data is important both for legal theory and for the state of the field. We must first know what ideals have been professed by the international community—what have states said?—before comparing nonverbal practice. As Michael Schmitt asserts, "states [now] need to roll into the game and start firming up the norms."[39]

The UN Office for Disarmament Affairs maintains a listing of the views of member states, which includes reports by the Secretary General as well as direct submissions by states parties.[40] In 2016, nineteen states made statements on the record, more than double than did in 2015. These included a number of influential players—Australia, Canada, India, Japan, and the United Kingdom—but also many from the developing world. The Geneva Internet Platform's Digital Watch Observatory, in partnership with the Inter-

net Society, also maintains a collection of resources, including UN GGE reports and related General Assembly resolutions organized by year.[41]

Finally, the Carnegie Endowment for International Peace maintains a searchable "norms index," which the website describes as "track[ing] and compar[ing] the most important milestones in the negotiation and development of norms for state behavior in and through cyberspace."[42] Users can compare specific language from international declarations and other discourse on issues ranging from aspirational norms to threat perception. This project promises to be of significant value to policy researchers.

What does the record reveal about the state of the field? While more analysis is needed, it is possible to trace some broad themes. Since the Russian Federation first brought the issue of digital security to the UN General Assembly in 1998, the international debate has been divided into roughly two camps over the nature of cyber sovereignty.[43] Russia and China have cooperated closely on cyber norms since 2011, repeatedly reaffirming their shared vision in a series of joint statements that *The New York Times* branded a "nonaggression pact."[44,45]As Kristin Eichensehr succinctly writes, this camp "advocate[s] a sovereignty-based model of cyber governance that prioritizes state control," whereas the United States and its allies "argue that cyberspace should not be governed by states alone," but rather in conjunction with a multiplicity of stakeholders.[46]

Even as sovereignty has remained a sticking point, agreement has become increasingly possible on other types of norms. The UN GGE, a collection of representatives from 25 influential countries of "equitable geographic distribution," has met five times since 2004.[47] The GGE has progressively moved the debate forward—from discussions in 2005 to consensus reports in 2010 and 2013.[48] At the 2013 meeting, GGE members agreed that international law applies to cyberspace just as it does to other domains, although the precise implications of this admission were not discussed.[49] It also recognized that general IHL principles may in some cases apply, and that states retain territorial jurisdiction over cyber infrastructure.[50]

By 2015–2016, many onlookers became optimistic that a system of norms on several important issues was indeed coalescing.[51] The GGE and the Group of Twenty (G20) each produced consensus documents. The GGE report enumerated five "limiting norms" geared around the permissibility of conducting cyber warfare or knowingly allowing one's own cyber infrastructure to damage another state's, as well as six "positive duties" affirming the need for multilateral cooperation and information sharing in the event of an attack.[52] Likewise, the G20 communiqué suggested that industrial espionage was prohibited, in line with U.S. interests.[53] This enshrined a bilateral understanding reached between the U.S. and China earlier in 2015, in which Presidents Xi and Obama agreed to cooperate in four areas: (1) a joint commitment to norm-building, (2) anti-cybercrime dialogue, (3) abstaining from knowingly supporting cyber-theft of IP, and (4) providing timely responses to transnational investigations.[54] Finally, fora such as the NATO Cooperative Cyber Defense Center of Excellence's (CCDCOE) Cyber Conflict Conference welcomed input from a more diverse array of participants, including legal scholars from China.[55]

But what was *not* said in these discussions is as important as what *was* said.[56] While the 2015 GGE was hailed for its consensus over norms, its "progress on international law" has been described as "modest."[57] For example, agreement could not be reached at the 2015 GGE over language about Article 51, the exclusion of which, *Tallinn Manual* editor Michael Schmitt argues, is an "untenable notion as a matter of international law."[58] Then, as mentioned previously, in 2017, after expanding membership to 25 countries, the GGE suffered an embarrassing failure to reach consensus, ending (or at least stunting) its trajectory as the lead forum for multilateral cyber law discussions.

The 2017 GGE reportedly did make headway on a number of important issues, such as a definition for the "knowledge" requirement in the previous report's rule that "states should not knowingly allow their territory to be used for intentionally wrongful acts"; a proscription against "hackbacks" (offensive operations by private sector entities against suspected offenders); and a *de facto* categorization of the Domain Name System as critical infrastructure, off-limits to attack.[59] Agreement is said to have broken down over U.S. insistence that the Article 51 threshold should apply, at least in principle, to cyberattacks of a sufficient scale.[60] The U.S. government and Western observers were quick to blame Russia, China, and Cuba.[61] In her statements

at the UN, U.S. delegate Michele Markoff attributed the impasse to "the reluctance of a few participants to seriously engage on the mandate on international legal issues."[62] However, the United States' insistence on the application and scope of key issues like Article 51 is by no means new, suggesting that it may have played a key role in the decision to end the discussions prematurely.

The failure of the 2017 UNGGE is not cause to abandon hope of normative convergence. Persuasion and adoption, when they occur, are gradual processes, and setbacks are inevitable. But as James Lewis has said, "the world's a long way from agreeing on basic principles of cyber sovereignty and those principles may not be written on U.S. terms."[63] Moreover, concerns have been raised that recent State Department shakeups could diminish the United States' say on cyber norm evolution moving forward.[64] As participants in the 2017 SOTF conference noted, to ensure favorable norms, the United States must both *stake out* and *set* precedents over time. Participants argued that what matters is not simply persuading the world, but rather maintaining that persuasive position.

Aside from (or in lieu of) *expressed* norms, there has been progress—as well as some retrogress—in *behavioral* norms. Following the United States' 2014 indictment of five Chinese People's Liberation Army (PLA) officers, the threat of economic sanctions, the 2015 Rose Garden agreement, and the G20 agreement, suspected Chinese hacking activity appeared to sharply decline, according to a much-reported FireEye analysis (although it is not clear to China-watchers whether more cooperative patterns are a result of, or epiphenomenal to, the agreements).[65] If U.S. strategies were indeed effective in dealing with China, similar indictments made against suspected Russian Federal Security Service (FSB) officers in March 2017 may also have a stabilizing effect.[66]

Given the political challenges of multilateral dialogue, private sector and other nongovernmental advocates may play a significant role in shaping cyber law discourse. A number of notable companies, including Google and Microsoft, have already displayed leadership. In early 2017, Brad Smith, Microsoft's President and Chief Legal Officer, called for a "digital Geneva Convention."[67] Shortly thereafter, Google proposed a framework that would obviate the need for MLATs by allowing governments to request evidence directly from Internet companies.[68] Norm entrepreneurs, particularly those from the private sector, will play an increasingly large role in the years to come.

Finally, although global norms are ideal for a globalized Internet, regional cooperation has gained more ground. The 2016 Organization for Security and Cooperation in Europe (OSCE), following up on its 2013 accord,[69] established a network of confidence-building measures and crisis hotlines spanning 57 countries. Similarly, in 2017, the European Council agreed on a "cyber diplomacy toolbox" that purports to streamline joint European diplomatic responses to cyber threats.[70] Whether regional cooperation will harden political blocs instead of helping to diffuse norms is unknown, but some cooperation is better than none for security and stability.

Modern Hague and Geneva law governing conduct in wartime arose in the wake of terrible historical experiences from the Battle of Solferino through the Crimean War, the American Civil War, World War I, and World War II. Is a catastrophe required for the formation of cyber norms? When this question was posed to SOTF participants, their answer was a unanimous "no." Although urgency turns discourse into action, anticipation of a terrible experience may be enough to catalyze change. If states universally recognize that particular types of behavior would lead to catastrophe, norms proscribing such activities should be easy to arrive at. This may be the case for rules like those against attacking CERTs and critical infrastructure in peacetime, for example, which have not been seen as controversial. Of course, this optimism hinges on a model of foreign policy decisionmakers as rational calculators, an assumption that may not always match reality. Nor is there any guarantee that norms established during peacetime would, as one reviewer put it, "survive first contact" in wartime.

Because norms are often established through leadership,[71] shaping norms in domains where actions are inherently secret or covert remains much more difficult. Further complicating matters, cyberspace has multiple stakeholders; most of the infrastructure and operators are nongovernmental. As a result, governments have only an indirect say over many behaviors, limiting their autonomy in this role.

Mistrust remains high. Despite China's apparent cooperativeness, one participant claimed that U.S. government insiders remain skeptical. There was also serious divergence throughout the room on the utility of the 2015 Rose Garden agreement,[72] with one participant arguing it was "100 percent a loss for the United States [and a] coup for China." Other participants were more optimistic, maintaining that, because the downturn in hacking trends appears to predate the agreement, indictments, or threat of sanctions, China's cooperation must be in its own interest. To realists and idealists alike, nothing is more stable than cooperation through mutual self-interest, at least until those interests change. The key may therefore be to codify law that aligns with the mutual self-interest of the most powerful states in the cyber domain, then shapes and constrains behavior even when those interests change.

Emerging Issues

Given the time constraints of the SOTF conference and the salience of particular topics, it was impossible to explore the full spectrum of legal and ethical issues that touch on cyberspace. However, some effort was devoted to brainstorming issues that may be of increasing importance in the years to come, for discussion at future SOTF workshops. First, although its use has evidently decreased in recent years, cyber network espionage (CNE)—especially industrial—will remain a hot-button issue. The *Tallinn Manual 2.0* discusses the issue at length, with no consensus about its permissibility at high levels. Widespread consensus holds that espionage, broadly, is not a violation of international law, but merely the domestic law of the target state (discussed more below). Cyber has made it increasingly possible for states to spy on entities outside the scope of traditional intelligence targets, such as foreign corporations. This has understandably given rise to heightened concern, particularly for high-tech, industrialized economies like the United States.

Unlike use of force issues involving computer network *attacks* (CNA), the debate over CNE norms has the potential to cut across traditional political divides. Even some Western countries do not share the U.S. view that the state and markets should be strictly compartmentalized and so, by logical extension, should their secrets.[73] However, the political consequences of being "for" industrial espionage are grave, creating a normative wedge whereby only the "against" side is vocal. In international law, silence can count as acquiescence.

Conventional espionage is normatively accepted between adversaries, and there is no international law proscribing it. As one participant put it, "espionage is more of an offense than a violation of anything." But in cyber operations, in the U.S. domestic law context, Title 10 (military) and Title 50 (intelligence and national security) roles are blurred.[74] And from the recipient's side, it is often hard to tell whether a system intrusion is an attempt to gather sensitive information or to plan an impending attack.[75] Although work has been done on the relationship between Title 10 and Title 50 in conventional spaces, there is a dearth of scholarly research on this dynamic in cyberspace.[76] The participants agreed that future SOTF workshops should consider U.S. national security law, broadly, without displacing the ongoing international law conversation.

Election influence or political inference is of obvious salience in the wake of the 2016 election. Cyber intelligence firm Crowdstrike released a report implicating Russian agents in a breach of Democratic National Committee (DNC) files shortly before the election.[77] About a month later, the U.S. Office of the Director of National Intelligence and the Department of Homeland Security stated that "the U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations."[78] In the time between then and the drafting of this report, Facebook surrendered information about 3,000 suspect advertisements to the U.S. Senate Intelligence Committee.[79] Similar concerns have arisen in other democracies: Emmanuel Macron, then a presidential candidate in France, had nine gigabytes of his emails leaked two days before the election.[80] Though repeatedly blamed, Russia is not the only source of such interference: online agitators from the United States were reportedly more culpable in interference with the 2017 German elections.[81] That the phenomenon of cyber interference in electoral politics has become routine not only provides a slew of case studies meriting deeper analysis, but also suggests the importance of this analysis for understanding issues like attribution, state responsibility, and sovereign non-interference.

Mass data breaches, ransomware, and other major cybercrimes are another topic of importance. These attacks have become more threatening in recent years, as was illustrated poignantly in the 2015 Office of Personnel Management hack and again in the 2017 Equifax breach, which included the personally identifiable information of 21.5 million and 143 million Americans, respectively.[82] Related to this is the issue of public-private sector cooperation and information sharing, particularly as it relates to the vulnerabilities equities process (VEP). During his administration, President Obama exerted considerable effort to bridge the trust gap widened by the Snowden leaks between private industry and U.S. intelligence collection agencies.[83] President Trump has made similar overtures.[84] Yet, as the 2017 WannaCry leaks revealed, the National Security Administration (NSA) exploited a vulnerability it discovered in the Windows operating system rather than notifying Microsoft to patch it.[85] After hackers stole the NSA tool used to exploit Windows and made it available on the open market, it was employed around the world. Systems in dozens of countries, including British hospitals and the Russian Interior Ministry, were infected. Despite the need for offensive capabilities, governments cannot treat cooperation as a one-way street and expect trust to be repaired. A 2017 U.S. Senate bill, the Protecting Our Ability to Counter Hacking Act of 2017 (PATCH Act), is one proposal to optimize this tradeoff by subjecting each new discovery to review.[86]

Given that artificial intelligence, autonomous systems, and the Internet of Things may all become more pervasive, some participants criticized *Tallinn 2.0* for focusing excessively on the human element. What ethical issues arise around self-executing, intelligent programs that remove human beings from the loop? How do they fit into the threshold debate portrayed in Figure 1?

Finally, because it may not be possible to say anything new about the "use of force" debate at the next SOTF conference, barring new and unexpected developments,[87] designating "sovereignty" as the umbrella topic might prove more fruitful. Beyond its public international law ramifications, sovereignty touches upon and could usher in subtopics that have thus far been overlooked in the SOTF forum: human rights law, domestic surveillance, comparative national security law, and public-private relations. These issues are all on a minable research frontier.

Summary & Recommendations

The past few years have been full of surprises. The world achieved a measure of cooperation on one major issue (economic espionage), lost it on another (the UNGGE), and witnessed the rise of new cyber threats (election interference). It is difficult to say where cyber norms are headed from here. Participants at the conference recalled "The Five Futures of Cyber Conflict and Cooperation," a 2011 article by Jason Healey. In it, the author imagines five potential futures—status quo, conflict domain, balkanization, paradise, and cybergeddon—assessing the nature, stability, intensity, and likelihood of each.[88] His conclusions are grim, but not dire: status quo or low-level conflict is likeliest, and cyber will continue to support a range of activities, both malevolent and benign. In 2018, is it reasonable to have the same expectations, or should we assign new probabilities to these potential futures? The participants were not able to reach consensus, but it was a useful thought exercise. Importantly, it highlighted that in each of the five potential futures, the law and ethics of cyber operations look very different.

The logical next question was to ask what the optimal U.S. grand strategy for cyberspace would be. In one participant's words, "which future should the United States be doubling down on?" Participants asserted that when the domain was in its nascent stages, the United States had an insurmountable lead in manpower, infrastructure, and companies; it built everything about the Internet. That may no longer be the case—many Internet companies operate abroad, foreign governments are increasingly competitive, and even in American universities, a great many computer science students are foreign nationals.

A minority of participants argued that the private sector is "still living in the Golden Days" of the past and fails to see the big picture. Balkanization is the future because it is the "min/max strategy" (that is, a strategy taken to minimize one's own maximum loss and maximize one's own minimum gain[89]) for states within which companies operate. A slim majority disagreed, arguing that because the private sector is globalized and profit-driven, it will align with whoever can make it money, putting bottom-up pressure on governments to keep online markets open. A small set of participants refuted this view by relating an anecdote about

the "PLA 5" indictments, discussed in brief earlier. These participants claimed that Pittsburgh industrial players, angry that the federal government had not adequately defended them from intrusions, persuaded U.S. Attorney David Hickton to "go rogue" in a fait accompli that was not wholly coordinated with main Justice Department or State Department priorities. By allowing the Western District of Pennsylvania to name the PLA 5, these participants alleged, companies knowingly sacrificed business in China. Other participants were unable to verify this account.

What if the upward trend in cyber norms really has been broken? Do we even need law, or are politics and strategy enough to sustain an uneasy peace, as they were during the Cold War? Several participants agreed that legal and ethical ambiguity has some merit, as uncomfortable as this assertion makes those who look to the law expecting clarity through bright-line rules. If the Article 51 line was known with certainty, states might be more willing to walk directly up to it without crossing. Absent this knowledge, they may find it safer to act conservatively and avoid provocation.

Finally, the working group uncovered several key issues on which more research is needed. First, a listing or map of MLATs—as well as more social science research on their causes and effects—would be helpful, given their proliferation and increasing importance in solving jurisdictional disputes. Second, given the state of the Article 51 debate, a next step might be to plot actual cyber incidents on the schematic in Figure 1. In so doing, researchers may be able to reverse-engineer behavioral norms and thus infer where states believe the red lines lie based on how they have behaved. Third, more attention should be paid to issues of domestic cyber law, including the blurred lines between military and intelligence operations; the emergence of national legal frameworks in the United States, China, Europe, and elsewhere in recent years; and human rights principles, from which the debate over IHL has detracted attention. Research on these topics would be of tremendous value to both cyber theorists and cyber practitioners.

About the Author

Justin Key Canfil is a Ph.D. Candidate within the Columbia University Department of Political Science.

End Notes

1. Schmitt, Michael N., ed. Tallinn Manual on the International Law Applicable to Cyber Warfare. Reprint edition. Cambridge University Press, 2013.
2. Cantwell, Douglas. "Legal and Ethical Issues." Cyber Conflict State of the Field Workshop Report. Cyber Conflict Studies Association, 2016, pg. 102.
3. Ibid., pg. 103.
4. Ibid., pg. 104, emphasis mine. Other recent works include Osula, Anna-Maria, and Henry Roigas, eds. International Cyber Norms: Legal, Policy, and Industry Perspectives. NATO Cooperative Cyber Defence Centre of Excellence, 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf
5. Cantwell, Ibid., pg. 105
6. Väljataga, Ann. "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly." NATO CCDCOE, September 1, 2017. https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html
7. See Maurer, Tim, and Kathryn Taylor. "Outlook on International Cyber Norms: Three Avenues for Future Progress." Just Security (blog), March 2, 2018. www.justsecurity.org/53329/outlook-international-cyber-norms-avenues-future-progress/
8. On this, see relevant research in progress by the author: Canfil, Justin Key. "Defense Divinations: The Design of International Contracts Under Uncertainty About Military Technological Change," presented at the 2018 International Studies Association (ISA) conference. Working paper available upon request.
9. "Cyber Operations and Cyber Terrorism." U.S. Army Training and Doctrine Command, Handbook No. 102. Fort Leavenworth, Kansas, August 15, 2005.
10. Waxman, Matthew. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." Yale Journal of International Law 36, no. 2 (January 1, 2011). http://digitalcommons.law.yale.edu/yjil/vol36/iss2/5
11. Katzenstein, Peter J. "Introduction: Alternative Perspectives on National Security." In Peter J. Katzenstein (ed.), The Culture of National Security: Norms and Identity in World Politics. Columbia University Press, 1996, pg. 5; North, D. Institutions, Institutional Change and Economic Performance. Cambridge University Press, 1990.
12. See, e.g., Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice, June 27, 1986.
13. See also Healey, Jason. "The Spectrum of National Responsibility for Cyberattacks." Brown Journal of World Affairs 18, no. 1 (Fall/Winter 2011); Lin, Herbert. "Attribution of Malicious Cyber Incidents: From Soup to Nuts." Journal of International Affairs 70, no. 1 (Winter 2016): 106.
14. Conventional sources are thought to include the 2001 International Law Commission's Draft Articles and ICJ caselaw; e.g. Corfu Channel, Iran Hostages, Tadic, Nuclear Weapons Advisory, Nicaragua, although primary sources per se are scant. See also notes from U.S. Cyber Command's "Cyberspace Operations in the Gray Zone" conference in February 2018: Adams, Michael J., and Megan Reiss. "International Law and Cyberspace: Evolving Views." Lawfare, March 4, 2018. www.lawfareblog.com/international-law-and-cyberspace-evolving-views
15. Ziolkowski, Katharina. "Customary Rules of International Environmental Law—Can They Provide Guidance for Developing a Peacetime Regime in Cyberspace?" In Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCD COE, 2013, pg. 135.
16. Ibid.
17. Refer to the chapter on attribution in this volume.
18. For existing research in this vein, see Canfil, Justin Key. "Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity." Journal of International Affairs 70, no. 1 (Winter 2016): 217–226.
19. McKay, Angela. "International Cybersecurity Norms." Microsoft. Accessed 2017.

20. McKay, Angela et al, "International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World," Microsoft, December 2014, pg 9.

21. Although c.f. proposals like the "accumulation doctrine": Ruys, Tom. The Intangible "Armed Attack": Evolutions in Customary Practice Pertaining to the Right of States to Self-Defence and the Quest for a Definition of "Armed Attack" Under Article 51 UN Charter. Proefschrift, 2009; Gervais, Michael. "Cyber Attacks and the Laws of War." Berkeley Journal of International Law 30 (2012): 525.

22. Rawlinson, Kevin. "Evidence Links China to GitHub Attack." BBC News, March 31, 2015, sec. Technology. www.bbc.com/news/technology-32138088

23. Convention on Cybercrime, ETS No.185, Budapest, November 23, 2001. www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

24. Boer, Lianne J. M. "'Echoes of Times Past': On the Paradoxical Nature of Article 2(4)." Journal of Conflict and Security Law 20, no. 1 (April 1, 2015): 5–26. doi:10.1093/jcsl/kru012; Hathaway, Oona, and Rebecca Crootof. "The Law of Cyber-Attack." Faculty Scholarship Series, January 1, 2012. http://digitalcommons.law.yale.edu/fss_papers/3852; Todd, Graham H. "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition Cyberlaw Edition." Air Force Law Review 64 (2009): 65–102.

25. Healey, Jason, and Hannah Pitts. "Applying International Environmental Legal Norms to Cyber Statecraft." I/S: A Journal of Law and Policy for the Information Society 8, no. 2 (2012); Marauhn, Thilo. "Customary Rules of International Environmental Law—Can They Provide Guidance for Developing a Peacetime Regime in Cyberspace?" In Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCD COE, 2013.

26. See, e.g., Gabcikovo-Nagymaros Project (Hungary/Slovakia), I.C.J. 7 (1997).

27. See Hollis, Duncan B. "Why States Need an International Law for Information Operations." Lewis & Clark Law Review 11 (2007).

28. Segal, Adam, and Matthew Waxman. "Why a Cybersecurity Treaty Is a Pipe Dream." CNN.com, October 27, 2011. http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/

29. Deeks, Ashley. "'Unwilling or Unable': Toward a Normative Framework for Extra-Territorial Self-Defense." Virginia Journal of International Law 52, no. 3 (August 2012): 483. https://ssrn.com/abstract=1971326

30. For a full exposition of countermeasures, see Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edition. Cambridge University Press, 2017.

31. Lotus judgment, at 23, quoted in "Jurisdiction," Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Ch 3. Cambridge University Press, 2013.

32. These jurisdictional bases include passive personality, universality, nationality, etc.

33. Lotus judgment, at 23, quoted in "Jurisdiction," Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Ch 3. Cambridge University Press, 2013.

34. Kraft, W., and Claudia Streit. "Ideas on the Establishment of an International Court for Cyber Crime." World Council for Law Firms and Justice, 2011; Choudhury, Rajarshi Rai, Somnath Basak, and Digbijay Guha. "Cyber Crimes-Challenges & Solutions. " International Journal of Computer Science and Information Technologies 4.5 (2013).

35. Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. Information Warfare and International Law. National Defense University Press, 1998; Kelsey, Jeffrey T. G. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare." Michigan Law Review 106, no. 7 (May 2008): 1427–1451; Cook, James L. "Is there anything morally special about cyberwar?" In Ohlin, Jens David, Claire Oakes Finkelstein, and Kevin Govern (eds.), Cyberwar: Law and Ethics for Virtual Conflicts. Oxford University Press, 2015.

36. Dinstein, Yoram. "The Principle of Distinction and Cyber War in International Armed Conflicts." Journal of Conflict and Security Law 17, no. 2 (July 1, 2012): 261–277; Schmitt, Michael N. "The Law of Cyber Warfare: Quo Vadis." Stanford Law & Policy Review 25 (2014): 269; Schmitt, Michael N. "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. " Harvard National Security Journal 8 (2017): 239–426.

37. Aldrich, Richard W. "The International Legal Implications of Information Warfare." No. INSS-OP-9. Air Force Academy, Colorado Springs, CO, 1996; Turns, David. "Cyber Warfare and the Notion of Direct Participation in Hostilities." Journal of Conflict and Security Law 17, no. 2 (2012): 279–297; Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." Berkeley Journal of International Law 27 (2009): 192; Asslani, Jabbar. "Study on the Legal Dimensions of the Cyber Attacks from IHL Perspective Abstracts." International Studies Journal 10 (2013–2014): I–XIII; Arimatsu, Louise. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations." In 4th International Conference on Cyber Conflict, pp. 1–19. IEEE, 2012; Droege, Cordula. "Get off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians." International Review of the Red Cross (2012); Geiß, Robin, and Henning Lahmann. "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space." Israel Law Review 45, no. 3 (2012): 381–399; Dunlap, Charles. "Perspectives for Cyber Strategists on Law for Cyberwar." Strategic Studies Quarterly (January 2011): 81–99.

38. *Hors de combat*, literally meaning "outside the fight" is a term of art referring to noncombatants, including prisoners of war, the sick and wounded, and unarmed civilians.

39. Quoted by Ansley, Rachel. "Tallinn Manual 2.0: Defending Cyberspace." Atlantic Council. Accessed September 26, 2017. www.atlanticcouncil.org/blogs/new-atlanticist/tallinn-manual-2-0-defending-cyberspace

40. "Developments in the Field of Information and Telecommunications in the Context of International Security." United Nations Office for Disarmament Affairs. www.un.org/disarmament/topics/informationsecurity/

41. "UN GGE." Geneva Internet Platform Digital Watch Observatory. https://dig.watch/processes/ungge#Resorces

42. "Cyber Norms Index." Carnegie Endowment for International Peace. http://carnegieendowment.org/publications/interactive/cybernorms

43. United National General Assembly Resolution 53/70. January 4, 1999. www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70

44. See Letter of September 12, 2011, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf; Letter of January 9, 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf; Roth, Andrew. "Russia and China Sign Cooperation Pacts." The New York Times, May 8, 2015. However, c.f. Davidson, Lincoln. "Despite Cyber Agreements, Russia and China Are Not as Close as You Think." Council on Foreign Relations, June 30, 2016.

45. "China, Russia Sign Joint Statement on Strengthening Global Strategic Stability." Xinhua News, June 2016. http://news.xinhuanet.com/english/2016-06/26/c_135466187.htm

46. Eichensehr, Kristen E. "The Cyber-Law of Nations." Georgetown Law Journal 103 (2015). https://georgetownlawjournal.org/articles/63/cyber-law-of-nations

47. "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law." CCDCOE, August 31, 2015. www.ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0

48. Grisby, Alex. "The UN GGE on Cybersecurity: What is the UN's Role?" Council on Foreign Relations, April 15, 2015.

49. Marks, Joseph. "UN Body Agrees to U.S. Norms in Cyberspace." Politico. Accessed September 26, 2017.

50. Schmitt, Michael, and Liis Vihul. "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms." Just Security, June 30, 2017.

51. Healey, Jason, and Tim Maurer. "What It'll Take to Forge Peace in Cyberspace." Carnegie Endowment for International Peace, March 20, 2017. See also, Maurer, Tim. "Cyber Norm Emergence at the United Nations." Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project. Harvard Belfer Center, September 2011; and Finnemore, Martha, and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." American Journal of International Law 110, no. 3 (July 2016).

52. "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law." CCDCOE, August 31, 2015.

53. "No country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." G20 Leaders' Communiqué, Antalya Summit, November 15-16, 2015, pg. 26. www.mofa.go.jp/files/000111117.pdf

54. Nakashima, Ellen, and Steven Mufson. "The U.S. and China Agree Not to Conduct Economic Espionage in Cyberspace." Washington Post, September 25, 2015, sec. National Security. www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html

55. Professor Huang Zhi Xiong from Wuhan University was invited to provide comments on Tallinn Manual 1.0, according to Deeks, Ashley. "Tallinn 2.0 and a Chinese View on the Tallinn Process." Lawfare, May 31, 2015.

56. See comments by James Lewis, quoted in Marks, Ibid.

57. Korzak, Elaine. "UN GGE on Cybersecurity: The End of an Era?" The Diplomat, July 31, 2017; Korzak, Elaine. "International Law and the UN GGE Report on Information Security." Just Security, December 2, 2015. www.justsecurity.org/28062/international-law-gge-report-information-security/

58. James Lewis, quoted in Marks, Ibid.; Schmitt and Vihul, Ibid.

59. Sukumar, Arun Mohan. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" Lawfare, July 4, 2017.

60. Ibid.

61. Korzak, Elaine. "UN GGE on Cybersecurity: The End of an Era?" Ibid.

62. Markoff, Michele. "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security." Remarks delivered to the United Nations, June 23, 2017. https://usun.state.gov/remarks/7880

63. Marks, Ibid.

64. Jason Healey, quoted in Starks, Tim. "Top State Cyber Official to Exit, Leaving Myriad Questions." Politico. Accessed September 26, 2017. http://politi.co/2vdSHtx

65. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Department of Justice Office of Public Affairs Press Release, May 19, 2014; "Red Line Drawn: China Recalculates its Use of Cyber Operations." FireEye iSight Intelligence, June 2016.

66. "U.S. Charges Russian FSB Officers and their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts." Department of Justice Office of Public Affairs Press Release, March 15, 2017. Although c.f. comments by James Lewis, who argues that Beijing may be uniquely susceptible to "naming and shaming" tactics: Groll, Elias. "DOJ Charges Russian Intelligence in Huge Yahoo Hack." Foreign Policy (blog), March 15, 2017. https://foreignpolicy.com/2017/03/15/doj-charges-russian-intelligence-in-huge-yahoo-hack/

67. Smith, Brad. "The Need for a Digital Geneva Convention." Microsoft on the Issues, February 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

68. Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era. Google, 2017.

69. Annual Report. Organization for Security and Co-Operation in Europe, 2013. www.osce.org/secretariat/116947?download=true

70. "Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions." Council of the European Union Press Release. June 19, 2017. www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/

71. For example, norms on nuclear weapons in space, customary international law on continental shelf maritime boundaries, and norms regarding satellite overflight.

72. Davis, Julie Hirschfeld, and David E. Sanger. "Obama and Xi Jinping of China Agree to Steps on Cybertheft." The New York Times, September 25, 2015, sec. Asia Pacific. www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html

73. Canfil, Justin Key. "Cyber Security and the Law: Managing Cyber Risk." 2014 Conference Report. The French-American Foundation, 2015.

74. Wall, Andru E. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." Harvard Law School, 2011.

75. Title 10 of the U.S. Code refers to the military operational side, whereas Title 50 encompasses intelligence operations.

76. e.g. Wall, Andru E. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." Harvard Law School, 2011. For an important exception regarding cyberspace law, see Chesney, Robert. "Offensive Cyberspace Operations, the NDAA, and the Title 10-Title 50 Debate." Lawfare, December 14, 2011. www.lawfareblog.com/offensive-cyberspace-operations-ndaa-and-title-10-title-50-debate

77. Bump, Philip. "Here's the Public Evidence that Supports the Idea that Russia Interfered in the 2016 Election." Washington Post, July 6, 2017.

78. Ibid.

79. Campbell, Barbara. "Facebook to Turn Over 3,000 Ads to Congress in Russian Election Interference Probe." NPR.org, September 21, 2017.

80. Greenberg, Andy. "NSA Director Confirms that Russia Really Did Hack the French Election." Wired, May 9, 2017.

81. Hjelmgaard, Kim. "There is Meddling in Germany's Election—Not by Russia, but by U.S. Right Wing." USA Today, September 20, 2017.

82. Nakashima, Ellen. "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say." Washington Post, July 9, 2015; Barrett, Devlin. "Chinese National Arrested for Allegedly Using Malware Linked to OPM Hack." Washington Post, August 24, 2017; Gressin, Seena. "The Equifax Data Breach: What to Do." Federal Trade Commission, September 8, 2017.

83. Segal, Adam. "Rebuilding Trust Between Silicon Valley and Washington." Council on Foreign Relations. Accessed September 26, 2017.

84. Cherelus, Gina, and Dustin Volz. "Trump Meets Silicon Valley Elite after Mutual Mistrust in Campaign." Reuters, December 15, 2016.

85. Brandom, Russell. "The NSA's Leaked Windows Hack Caused More Damage than Just WannaCry." The Verge, May 17, 2017. www.theverge.com/2017/5/17/15655484/wannacry-variants-bitcoin-monero-adylkuzz-cryptocurrency-mining

86. Protecting Our Ability to Counter Hacking Act of 2017, U.S. Senate, 115th Congress, 1st Session. www.schatz.senate.gov/imo/media/doc/BAG17434_FINAL%20PATCH.pdf

87. C.f. Goodman, Ryan. "Cyber Operations and the U.S. Definition of 'Armed Attack.'" Just Security (blog), March 8, 2018. www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/.

88. Healey, Jason. "The Five Futures of Cyber Conflict and Cooperation." Georgetown Journal of International Affairs (2011): 110–117.

89. Definition from Hammoud, Naima, "Game Theory: Minimax, Maximin, and Iterated Removal," lecture slides. University of Oxford, March 14, 2017.

The Cyber Conflict Studies Association (CCSA) promotes and leads international intellectual development efforts to advance the field of cyber conflict research. These activities include workshops that bring together professionals from industry, academia and government to discuss strategic issues surrounding cyber conflict and the publication of insightful research articles and position papers and books. CCSA also plays an important role in our national cyber-readiness strategy, serving as a resource for national security decision-makers and helping to frame and promote national cyber conflict policy. CCSA brings together the best and the brightest individuals in the field of cyber conflict study to further the goals of national security and the field of cyber.

This work was supported in part by the Minerva Research Initiative. The Minerva Research Initiative, administered jointly by the Office of Basic Research and the Office of Policy at the U.S. Department of Defense, supports social science research aimed at improving our basic understanding of security.

Funded in part by the Office Naval Research under the OSD Minerva program, grant number: N00014-17-1-2423.