JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2021, 1–9
doi: 10.1093/cybsec/tyab009
Research Paper

Research Paper

Why international law and norms do little in preventing non-state cyber attacks

Nori Katagiri *

Department of Political Science, Saint Louis University, McGannon Hall 152, 3750 Lindell Boulevard, St Louis, MO 63108, USA

*Correspondence address. Department of Political Science, Saint Louis University, McGannon Hall 152, 3750 Lindell Boulevard, St Louis, MO 63108, USA. Tel: +1-314-977-1462; E-mail: nori.katagiri@slu.edu

Received 26 May 2020; revised 5 February 2021; accepted 18 February 2021

Abstract

In this article, I investigate why international law and norms have failed to keep cyberspace peaceful. The problem comes mainly from their failure to address what non-state actors, such as individual hackers and technology firms, do in cyberspace. Created by the extensive input of government officials decades ago with heavy focus on states as primary actors of international politics, international law is incoherent with the dominance of non-state actors as *de facto* operators of cyberspace. The critical problem shared by international law and institutions of having no "teeth" to penalize non-state violence extends to cyberspace. As a result, noncompliance with international law has become practical, and it has even bolstered the private sector, especially major technology firms, to assert themselves in the legal void, leverage their digital products to reshape norms, and become norm entrepreneurs in the business of digital defense. However, the multiplication of norm entrepreneurs has accelerated in an uncoordinated manner, and the way they built their interests does not neatly align with those of the states. While some norms of cyberspace behavior have been accepted, many others remain contested. In the meantime, norm discourse in diplomatic venues, including in multilateral debates at the United Nations, has become highly undemocratic, dominated by a small mix of great powers and active middle powers that are also split over what norms should guide state and nonstate behaviors.

Key words: international law; cyber norms; democracy; nonstate actors

Introduction

The Coronavirus Disease 2019 (COVID-19) outbreak was a sudden blessing to cyber warriors looking for opportunities to trick people with scams and malware. Hackers capitalized on the pandemic by "registering malicious coronavirus-related domains, selling discounted off-the-shelf malware on the dark web", and sneaking into networks of people forced to log on from home. By March 2020, the number of new domains designed to profit off the global health concern increased 10-fold the average number of previous weeks, along with an uptick in the number of phishing emails thrown at hospitals and virus testing facilities. At one point, an Android app called CovidLock promised to deliver the latest information on the pandemic, only to lock up a user's phone with a strain of malicious software and demand ransom of $100 in bitcoin to be paid within 48 h of infection [1]. At another time, Pakistan's state-sponsored threat actor called APT36 ran "a spear-phishing campaign using COVID-themed documents that masqueraded as health advisories to deploy the Crimson Remote Administration Tool onto target systems" [2].

It was a familiar picture for most observers of international security in times of crisis; national governments scrambling to protect their networks, private firms recovering from damages, and insurers looking for every excuse to raise premiums. One fact emerged: victims received little to no visible protection from international institutions, laws, or norms of cyberspace behavior. The United Nations called for collective action on the coronavirus, but none on cyberattacks, and no international institution stood up to defend cyberspace during the crisis. Some existing norms of behavior, ranging from responsible state behavior to the ban on deliberate attacks on civilians,

went completely ignored. More importantly, the pandemic reminded us of the broader reality in international politics about cyber anarchy in full swing; international law, institutions, and norms continue to play a limited role in preventing nonstate cyberattacks. While some believe that institutions are necessary to prevent cyberattacks because they promote the rule of law and peaceful use of cyberspace and impose reputational costs on malicious actors [3]. It remains true that international law and norms have done little to prevent cyberattacks by nonstate actors. There is no international treaty on cyber operations by these actors, nor is there a consensus among stakeholders that we need one. In this context, what is missing from the literature is a critical assessment of why international law and norms have done little to prevent nonstate attacks on states. In this article, I seek to offer one.

My argument is as follows. Despite much attention they garnered, international law and norms have failed to keep cyberspace peaceful. The problem comes mainly from their failure to address what nonstate actors, such as individual hackers and technology firms, do in cyberspace. Created by the extensive input of government officials decades ago with heavy focus on states as primary actors of international politics, international law is incoherent with the dominance of nonstate actors as *de facto* operators of cyberspace. The critical problem shared by international law and institutions of having no "teeth" to penalize nonstate violence extends to cyberspace. As a result, noncompliance with international law has become practical, and it has even bolstered the private sector, especially major technology firms, to assert themselves in the legal void, leverage their digital products to reshape norms, and become norm entrepreneurs in the business of digital defense. However, the multiplication of norm entrepreneurs has accelerated in an uncoordinated manner, and the way they built their interests does not neatly align with those of states. While some norms of cyberspace behavior have been accepted, many others remain contested. In the meantime, norm discourse in diplomatic venues, including in multilateral debates at the United Nations, has become highly undemocratic, dominated by a small mix of great powers and active middle powers that are also split over what norms should guide state and nonstate behaviors.

In this article, I define a cyber attack following Herbert Lin as "use of deliberate actions and operations … to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information." I treat cyber attacks as equivalent to offensive cyber operations (OCOs) [4]. This article proceeds in four steps. First, I point out several flaws in international law as a major cause of its failure to address cyberspace insecurity, especially issues related to nonstate actors. Second, I explore a set of norms and principles of cyberspace behavior to show how some of them have failed to address nonstate cyberattacks. Third, I examine the disruptive role of these actors, especially private technology firms, in the norm discourse under a defunct legal system. Fourth, I show how state disagreement has hampered the norm discourse.

Problems with international law in preventing nonstate cyberattacks

Scholars who stress the centrality of international law and institutions in cyberspace insist that they have enough power to curb the proliferation of cyber attacks. Their optimism has increased in the past decade with a succession of international agreements to accelerate rule-based collaboration to reduce malicious activities. International institutions have encouraged the proliferation of democratic norms across states and socially penalized incompliant states [5]. Legal scholars have published a number of works on many aspects of cybersecurity, claiming how international law may apply to cyberspace and constrain cyber attacks [6–9]. The optimism reached its pinnacle in the publication of the Tallinn Manuals, written by a group of scholars collectively called the International Group of Experts (IGEs) who have set the tone of academic discourse on the application of international law to cyberspace [10].

Because they tend to focus on *how* law may apply to cyberspace rather than whether, they are largely blind to the flaws that make the application difficult. Enough scholarship has shown over the years that international institutions, which govern international law, are notoriously ineffective when it comes to regulating interstate violence. Worse, they are even less effective against nonstate cyberattackers because it is hard to observe covert actions and because the institutions generally lack the authority to enforce rules of law on nonstate actors. Officials and scholars have found institutions useful mostly for the powerful states that run the very institutions and execute their will on the less powerful. When it comes to preventing nonstate attacks, major powers acknowledge that international institutions are less useful, which explains why few, if any, states have resorted to the institutions for help with fending off OCO during the COVID pandemic. This comes in part from the legal scholars' narrative that international law shall only address states at the exclusion of nonstate actors. Schmitt and Watts claim that "The public international law principles and rules bequeathed by preceding sovereigns remain intently focused on the interactions of states. International law places states at the center of its legal regimes" [11]. The scholars also willingly interpret international law in ways that give states an advantage over nonstate actors in cyberspace. They write that "Non-state actors are fully subject to states' exercises of sovereignty" such that they are not even allowed, as if they were required to be, to take countermeasures for self-defense because "such measures are a response reserved to states" [11]. This approach to international law faces the problem of nonrelevance in the cyber age when nonstate actors are as active as states. In fact, legal scholars concede that the power of international law to regulate nonstate actions is limited. Schmitt and Watts admit that "the law as to when an operation against a non-state actor violates the sovereignty of the state where that actor is located is unclear. … While cyber operations by a state may violate the sovereignty of the state where the non-state actors are located, cyber operations by non-state actors that are not attributable to a state as described below do not constitute a violation of sovereignty" [11].

The mainstream view of international law faces some skepticism of its own. Examining the initial reactions of states to the publication of the Tallinn Manuals, Dan Efrony, and Yuval Shany find it "difficult to ascertain whether states accept the Tallinn Rules and wish them to become authoritative articulations of international law governing cyber operations," questioning "the degree to which the Tallinn Rules are universally regarded as an acceptable basis for articulating the norms of international law governing cyber operations" [12]. Other legal scholars accuse the state-centric scholars of desperately "intervening" into areas they know law matters little. Jean d'Aspremont writes that these scholars "have considered that cyber operations have been left dangerously unregulated … In their eyes, such a situation is conducive to injustice and disorder. This is why, without awaiting any impulse or indication by international lawmakers, international lawyers have brashly seized themselves of the 'cyber problem' … to address such a legal vacuum with their own tools and ensure that cyber operations are subjected to international legal rules of which they are the experts" [13].

The failure of international law to address nonstate activities comes from three problems. The first is the lack of definitions of some of the most important operational concepts. To this day, states have never agreed to a common definition of "use of force" and "armed attack," among other terms, in the framework of international law, permitting interpretive differences to shape interstate negotiations. Legal scholars have subsequently failed to help fix the problem for states. Schmitt admits that the IGE has failed to generate agreeable definitions and instead decided to settle by offering "factors" that decision-makers are "likely" to consider, including severity, immediacy, invasiveness, and identity of attackers, and allowed states to determine the meaning of the terms their way [14]. Obviously, states ignore these and go with different standards, but the conceptual ambiguity has kept states from invoking an international set of standards to recognize a cyber attack as such. Consequently, no state but the USA has to date acknowledged a cyberattack as use of force. None has characterized the 2010 Stuxnet attack as the use of force because, as Heather Harrison Dinniss suspects, it did not result in the damage of *physical* property, injury, or loss of lives.[1] Without clearly defined terms, no state can accuse others of an "internationally wrongful act," another undefined but widely used term among legal experts.

This problem has always been grave among states, but it becomes more so when it comes to state treatment of nonstate attackers. Even though the legality of self-defense centers on the definition of those terms, the blanket application of state-centric definitions to nonstate actors has brought about more confusion. This is because international law is considered "extendable" to nonstate actors when it does not address the degree to which nonstate actors are diverse. The application of international law to nonstate actors involved in cyber businesses, ranging from individual hackers to private firms to defense consultants, would require different standards for each. Yet, there is no standard that sovereigns have agreed.

Lack of conceptual clarity deepens the second, already severe problem of attribution in cyberspace. Although attribution is necessary for international law to establish facts and circumstances and to execute the rights and obligations of affected states, it does not automatically specify consequences for violators. There are no concrete standards in international law for producing sufficient evidence for states, let alone non-state attackers, to accuse each other of wrongdoing. Dennis Broeders, Els De Busser, and Patryk Pawlak write that the International Court of Justice claims to have adopted a "clear and convincing standard" for cyberspace attribution even though what that means exactly is still debated among legal scholars [15]. International law presents no specific rules on how much and what kind of evidence is enough for one to make a case on attribution. This problem has trickle-down effects on states; it has forced them to resort to nothing more than making broad statements of ad hoc condemnation. To date, no state has attributed an OCO through a clear reference to a rule of international law. Broeders, De Busser, and Pawlak conclude that "the absence of references to international law in the existing accusations also diminishes the value of international law as an instrument aimed at preventing conflict in cyberspace" [15].

It is even more difficult to establish an evidentiary link between states and nonstate actors who act as proxies for them, including advanced persistent threats (APTs).[2] The reason has much to do with the fact that international law writ large makes essentially no reference to the strategic environment in which a growing number of murky actors have served as state forces. This is a serious matter for many because states that are known to have aimed APT operations toward them have mostly been authoritarian states, especially the so-called "big four" – China, Russia, Iran, and North Korea. Attributing APT-borne OCO to their sponsors has been extremely difficult, and even when states do manage to trace OCO back to certain groups, there is no international legal standard to accuse the suspects through proper channels and place them on appropriate courses of action toward trial at international courts [16].

The final problem is that states have chosen not to subject themselves to international standards and instead have resorted to other options [8, 17, 18]. The bypassing is logical; existing law makes no clear conceptual and policy guidelines and extends neither penalty for violation nor incentives for compliance. In other words, states receive no legal protection from international institutions from cyberattacks by nonstate actors. While violators would face reputation costs and the risks of domestic political action [3], many care more about abusing the system for immediate gains. Some even welcome the opportunity to build their reputation via defiance of law. China knows that, for instance, defiance of the Western system often serves its political narrative, so it runs espionage campaigns against Western media critics, such as *The New York Times* and *The Washington Post*. Beijing has similarly coerced firms like Google and Facebook to submit backdoor security information in exchange for operating in its "cyber sovereignty." While China's actions may have weakened its soft power in general, they help strengthen its image [19]. Contrary to expectations, the reputational incentives actually make it hard to prevent violators from exploiting the flawed system.

Of course, the flaws in the law do not make cyberspace devoid of order. Order is given in part by existing institutional arrangements that offer a "patchwork" of separate regulations over issues like online crimes and attacks on telecommunications systems. In a way, compartmentalization is the way to go; it helps nations identify vulnerabilities and build a case for broader preventive mechanisms [20]. Yet, it does not relieve states' fear of commitment. For example, the 2001 Convention on Cybercrime is an international treaty that requires signatories to penalize illegal access, interception, and misuse of devices. As of February 2021, 65 nations were signatories to the so-called Budapest Convention. In other words, more than a majority of independent states in the world have failed or declined to ratify it for nearly 20 years since the Convention came into being. One of the problems with it is that it gives no clear law enforcement authority on data interception and network search, nor does it protect confidentiality and system integrity [21]. Another problem is that it has done little to restrict the diffusion of malicious software or regulate state actions with threats of penalty [8, 22]. Signatories have little incentive to honor the accord, and nonsignatories like Russia and China simply do what they want. Russia has rejected the Convention because it is unwilling to let its cyber criminals who operate against the West prosecuted [23]. In fact, Moscow garnered international support at the end of 2019 to create a different treaty on cybercrime. China, on the other hand, has stayed out of the Convention so as to continue regulating its cyber-sovereignty and back Russia's bid for the counter treaty.

In contrast to legal scholars, security scholars are overwhelmingly skeptical about the usefulness of international legal arrangements.

1 Heather Harrison Dinniss writes that "this attack is perhaps the clearest example to date of a computer network attack amounting to a use of force (if not an armed attack)" [7].

2 I define APTs as groups of hackers who conduct OCO on behalf of state sponsors in the form of espionage, data destruction, and online manipulation [16].

Most say that in cyberspace, defense is disfavored and deterrence ineffective against cyberattacks, with the assumption that institutions are no cure to this problem [24–26]. Existing institutions have had few enforcement, verification, or penal mechanisms in place, leaving everyone else to their own devices. I join the school of thought in asserting that international law does little to change the strategic landscape. In fact, I even go as far as to contend that the current legal framework, as applied to cyberspace, has made things worse for believers of international law due to its selective disassociation from the role that nonstate actors play in cyberspace. The main cause of the problem is the prevalence of state-centrism in the law and the lack of state commitment to reforming the system to reflect the greater role played by nonstate actors.

Growth of international norms to prevent cyberattacks

There is a close linkage between international law and norms. That is, if international law is ineffective in preventing cyberattacks, expectations are that social norms would do the job. If the legal exclusion of nonstate actors is what causes problems, norms should include them. A "standard of appropriate behavior for actors with a given identity" [27], norms and law are two different things, but in cyberspace they are inseparable. That is, failure of international law to address cyber vulnerability feeds into expectations that norms would do the job, while norms themselves are a function of the acceptance of international law applied to cyberspace. Certainly, they develop differently. People would accept law when there is a norm for it. They would have to agree with nonbinding norms before they sign binding treaties [28].[3] But ultimately, norm-making is complex; Martha Finnemore and Kathryn Sikkink show that norms must go through three stages to become legitimate. In the first phase of emergence, norm entrepreneurs with sufficient organizational platforms persuade enough people into agreeing with the norm to reach the "tipping point." The entrepreneurs (in this case, they include states and firms) then work with other actors like international organizations and NGOs to legitimize the norm. This forms the second process of socialization and institutionalization. Finally, the norms become embedded in society through the phase of internalization, which involves legal, professional, and bureaucratic processes of making them a human habit. In what they call the "life cycle" of norm-making, ideas that become norms are ones that are accepted through legitimation, socialization, and institutionalization [27].

Norms have risen to the occasion to fill the legal void in the regulation of OCO [17, 18]. Joseph Nye proposes that norms like taboos can deter cyber attacks and help stabilize cyberspace because they impose reputational costs on actors with malicious intent [3]. As such, some norms have been in operation for some time to incentivize peaceful behavior. They include confidence-building measures, capacity-building, efforts to refrain from targeting each other's community emergency response team, responsible state behavior, respect for sovereignty, peaceful settlement of disputes, noninterference into national cyberspace, bans on deliberate attacks on critical infrastructure, and promises of forensic assistance when needed. Many of these norms have been accepted and practiced over the years. For instance, despite the aforementioned large number of OCO on commercial apps, few states have been attacking each other's critical infrastructure. Most states limit their actions to probing target systems, leaving real attacks on civilian-based systems dramatically rare. These norms are particularly salient among states that behavior more consistent with the general rules of engagement than authoritarian states. As I discuss below, some of the ideas embedded in multi-stakeholder agreements like Microsoft's Cybersecurity Tech Accord have become norms that account for both state and nonstate actors.[4]

States have also worked in a variety of institutional settings to establish norms to prevent conflict, including the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace (GGE). GGE's role has been critical in raising the public awareness of norms in cyberspace, although it has no internationally recognized administrative power to enforce international law on state actions. Take, for instance, the 2015 GGE's recommendation of 11 "norms of responsible state behavior," a set of proposed principles of behavior that its members have agreed to, as seen in Table 1. There is no question that many of the norms have been honored by states. Yet, there are three problems with them. First, they are expressed in terms that are designed to enhance the "soft" impression of messaging to induce proactive compliance. The use of terms like "should" and "knowingly" in the statements, as in "states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" (recommendation 1), comes with the effect of toning down the weight of "responsible" state behavior. Phrases like this may generate a perverse effect of allowing states to essentially lie about their actions through the benefit of the doubt. Second, some ideas contained therein, like mutual respect for sovereignty and noninterference, have proven to be daily violated, especially by nonstate attackers. The expressions contained in Table 1 are designed to encourage otherwise noncompliant states to comply, but at the end of the day, they do not change the fact that states, which constitute the primary membership of the GGE, want to retain the power to undermine others' security. As a result, while there is a norm that compliance is desired, there is a norm that *in*compliance is the practice. If there is a norm that norms should be there, there is another norm that such norms be low-hanging fruits. This problem becomes acute when we consider the fact that the norms are explicitly addressed for state audiences and have little to say about nonstate actors. This is consistent with the existing problems of international law which has excluded the role played by nonstate actors.

The norm regime has grown along with the contestation of discourse. That is, some norms that are considered "accepted" have become subject to contestation. Take, for instance, the notion of "ethical" hacking – the act of helping identify software and network vulnerabilities by doing things like penetration testing and red teaming. For sure, these ethical works are socially accepted and have transformed into a consultation industry. In 2019, Google paid out over $6.5 million in rewards to a total of 461 white-hat hackers, a record-high amount that was twice as large as the previous year [29]. But white-hat hackers have never dominated the marketplace of ideas; instead, they have faced off with black-hat rivals, with undecided "gray-hat" hackers being swing voters. The norm contestation is fueled by the rapid inflow of financial incentives. Hackers remove their black gloves when lured by government officials and recruiters who pay enormously to defend their systems. Black-hat hackers are motivated by both financial gains and social injustice, but they may turn white if the bounty becomes too attractive.

3 Nye writes that in cyberspace, "a binding international legal treaty would be premature as the next step [28].

4 I thank the reviewers for raising this point.

Table 1. GGE's cyber "norms of responsible state behavior" in 2015

	Recommended norms	Evaluation
1	States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (Information Communication Technologies)	Terms like "should" and "knowingly" help increase the chance that the norm is honored by lowering the bar of compliance Norm has nothing to say about nonstate actors
2	States should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure	Same as above
3	States should take steps to ensure supply chain security and seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions	Most states honor the norm; norm has nothing to say about nonstate actors
4	States should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity	Terms like "should" and "knowingly" help increase the chance that the norm is honored by lowering the bar of compliance; norm has nothing to say about nonstate actors
5	States should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age	Same as above, although many rights, including privacy and right of expression, have been violated
6	States should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices	Most states honor the norm; norm has nothing to say about nonstate actors
7	States should consider all relevant information in case of ICT incidents	Most states honor the norm; norm has nothing to say about nonstate actors
8	States should consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs	Most states honor the norm; norm has nothing to say about nonstate actors
9	States should take appropriate measures to protect their critical infrastructure	Most states honor the norm; norm has nothing to say about nonstate actors
10	States should respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts	Most states honor the norm
11	States should encourage responsible reporting of ICT vulnerabilities and should share remedies to these	Most states follow the norm

The NATO Cooperative Cyber Defence Centre of Excellence, 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law.

Norms of legal principles in cyberspace

To illustrate how some norms are contested, I discuss three principles of international legal behavior – (i) application of international law to cyberspace and the principles of (ii) distinction and (iii) proportionality. The first principle is the most well-known principle that states have agreed to, and the other three are drawn from existing international law and applied to cyberspace. First, the notion that "international law is applicable to cyberspace" has achieved wide acceptance since the 2013 GGE. The notion concerns the UN Charter, Article 2(4), which bans the threat or use of force and calls on member states to respect the sovereignty and territorial integrity of each other. Although the article does not address cybersecurity per se, it is understood that member states treat cyber attacks that leave physical damage as use of force. (Rule 69 of the Tallinn Manual 2.0 states that a cyber operation "constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of "force" " [30, 31]. As such, the article could be used to hold violators accountable if Member States present material evidence of damage. The problem, however, is that the term "use of force" is nowhere defined in international law. Because it is unclear under what conditions a cyberattack becomes use of force, the Article establishes no automatic punishment or enforcement standard. Without such a standard, the principle renders enforcement a political process. The problem becomes acute when it comes to nonstate actors; as I demonstrated above, no international law explicitly addresses to nonstate cyber actors. This means that not only international law but also the norm that underscores it fails to extend behavioral restrictions on nonstate cyberattacks.

For a principle like this to prevent cyberattacks, states must be able to identify and verify violations of the norm. To identify violations and attribute a cyberattack to a perpetrator is known to be hard, but even if attribution is correctly made, there are at least three problems with the process of verification. First, there is no international body with a mandate to oversee nonstate cyber operations and enforce states' will to punish perpetrators. It is left to individual states to conduct such a task, which in turn reinforces state-centrism at the cost of international cooperation. Any country that gets to run the body, however it may be selected to do so, would have incentives to abuse the power that comes with it to hide its own adventure. This is in part because there are a number of nonstate agents operating on states' behalf. So the system is designed to impede international coordination at this point. Second, verification of violation is hard because victims often want to keep incidents secret to avoid embarrassment and loss of credibility. Victim states gain little for standing up to perpetrators when there is no objective body to penalize the latter. This problem is salient for leaders who face elections in the near future. Finally, nonstate attackers can complicate attribution to undermine the verification and enforcement processes. They can do so by, for instance, launching OCO via multiple platforms and hiring proxies that impersonate third parties to disguise operations. There are simply too many things that nonstate attackers can do to hinder the verification process; as such, no state has stepped forward with sufficient evidence to trigger the UN Charter Article 2(4) or pursued perpetrators to prosecute in international courts.

If the normative application of international law does not work, states would hope that other principles of behavior would help constrain nonstate attackers. One of the most important principles is that of target distinction, under which states are obligated to choose targets based on differences between civilian and military objects. Under international law, only military objects can be targeted in "traditional" conflict settings, and such an object is considered

visible. But there are two problems with executing the principle in cyberspace. First, the fact that much of cyberspace is dual-use hinders distinction. Take data for example. The former US Secretary of Homeland Security, Michael Chertoff writes that "(t)he digital packets flowing over the infrastructure may simultaneously include military and civilian data elements. Logically, one might argue that the entire internet, or a substantial portion, is a military object" [32]. States could try to protect dual-use objects from OCO by designating them as environmental and cultural installations under "special protection," but the standard for designating objects as such remains inadequately clear [7]. No one is authorized to enforce the special protection, and the conditions under which penalty can be imposed upon violators are unclear. Second, the distinction principle does little to constrain nonstate attackers. Having nothing to say about such actors, the principle accords a great deal of operational freedom. This is one of the reasons why nonstate actors have successfully compromised many commercial apps, civilian data centers, and medical facilities over the years.

The other principle is that of proportionality, a notion that active defense retaliation, permissible under customary international law, warrants retaliation that is proportional to the first strike. In cyberspace, the problem is that no law or norm clarifies how to measure proportionality [24, 33]. This allows states to measure proportionality in their own way, which deepens the problem. That is, a lack of clarity over measurement raises the chance that retaliation would be perceived differently than the original intent. The difference in the perception of proportionality, which Henry Farrell and Charles Glaser call the "salience gap," increases the probability of misunderstanding between the attacker and retaliator [34]. Misperception can lead to an unintended escalation in two ways. On the one hand, one may launch a countermeasure that ends up "overshooting" the target, forcing the latter to consider the measure excessive. Overshooting results from a gap in mutually acceptable levels of proportionality and can result in the escalation of tension if it causes the victim to retaliate. Overshooting is a problem because it affects operators' readiness by instilling fear that they would be held accountable for causing more damage than intended [34]. On the other hand, if the retaliation does not stop the attacks, operators may conclude that their action has "undershot" the aim. The undershooting of the target would require additional action (a follow-on attack) to get even when doing so may push up the threshold of real proportionality, leading to overshooting (and escalation). The follow-on attack can make things worse because once the target gets the first shot, it is likely to make adjustments and upgrade the defense system, forcing the attacker to look for the next vulnerabilities in search of the "right" level of proportionality.

If states do not care for the principle, neither do nonstate actors. It is not hard to imagine that the principle is routinely dishonored by hackers and firms, especially those that provide the digital infrastructure itself. Firms may act on due diligence in at least three different ways. First, they may shun states that practice due diligence to protect their operations and profit. Second, some firms may fail to practice due diligence, making states that work with them culpable as a result. Third, some firms may shun states that do not practice due diligence, because they are concerned about their own vulnerability. This case is most likely with firms that work with subsidiaries that are even more vulnerable. These subsidiaries, many of them small support firms, often lack resources and skills for self-defense and have themselves been attacked several times already, often without knowledge. Kevin Fahey, the US assistant secretary of defense for acquisition (2017–present), says that "big companies tend to give their smaller subcontractors a lot of data they don't need, which then becomes vulnerable to foreign hackers … our adversaries don't try to come in through the big companies, they come in through the fifth-, sixth-tier." In 2016, for example, foreign agents hacked US defense networks and stole sensitive data on the multinational F-35 jet program from an Australian subcontractor [35]. The problems with private actors demonstrate that the principle is prone to fail when digital infrastructure is deeply connected through various states and firms.

How norms permit nonstate attacks

Like international law, some cyberspace norms not only are ineffective but also condone nonstate attacks. The way they do so is mostly by negligence of states. State disagreement over international law and its normative application has induced the private sector, including major technology firms, to generate norms as part of corporate growth. With elevated status in the norm community and with significant stakes in the way cyberspace is governed, technology firms have formed alliances to increase collective voice. Varying in size and purpose, these alliances have multiplied in the democratization of the norm industry. Small groups like the Charter of Trust (17 companies led by Siemens) and Cyber Threat Alliance (26 led by Cisco) seek to achieve limited aims like sharing technical data about vulnerabilities to enhance collective information security. Small companies find it prudent to be part of these networks to keep abreast. But other firms have formed alliances of larger membership, like Microsoft's Cybersecurity Tech Accord with over 150 partners. They operate with greater intent to shape the future of digital safety, limit government use of private networks against citizens, and uphold values like corporate trust and social accountability [36].

Yet, the democratization of the norm industry is exactly what keeps norms from preventing cyber attacks. Table 2 below lists some of the best-known groups with a set of principles they have proposed. It indicates two characteristics. First, the principles are not consistent across alliances. Each alliance is a patchwork of major firms with different types of norm expectations and business interests. Furthermore, membership does not overlap most of the time; what we see instead is the multiplication of competing norm entrepreneurs. Second, some principles are more accepted in the digital community than others. Principles like "strong defense" and "capacity building" in the Cybersecurity Tech Accord and "unite global communities" and "implement concrete solutions" in the Global Cyber Alliance have become internalized, socialized, or institutionalized. Yet, others are contested, such as "transparency," "(private) ownership for cyber and IT security," and "regulatory framework" which are promoted by the Charter of Trust. These norms are likely to raise government objections even if ordinary citizens may find them acceptable. Even actions like "disrupt malicious activity by rapidly sharing intelligence" (Cyber Threat Alliance) can be controversial because, without government oversight, they would go against all sorts of national security procedures and intelligence protocols. Other ideas they promote have yet to be "normalized" in society at large. This stems in part from the fact that while firms have significant responsibility toward the public, they do not serve the public the way states do. Profit models often conflict with accountability and transparency.

There is no denying that these firms have grown influential. They have done so by seizing the advantage they have in using technological output as a means of shaping norms. But the problem is that norms grow more slowly than technologies. Firms produce IT products and services much faster than consumers fathom the

Table 2. Norm stakeholder groups and their principles (Information is as of 4, April 2020)

Name	Leader company	Member companies	Major principles
Charter of Trust (Charter of Trust, https://www.charteroftrust.com/)	Siemens	17	Ownership for cyber and IT security; responsibility throughout the digital supply chain; security by default; user-centricity; innovation and co-creation; education; Certification for critical infrastructure and solutions; transparency and response; regulatory framework; and joint initiatives
Cyber Threat Alliance (Cyber Threat Alliance, https://www.cyberthreatalliance.org/)	Cisco	26	Protect customers, critical infrastructure, and the digital ecosystem; prevent, identify, and disrupt malicious activity by rapidly sharing intelligence; reward context sharing; attribute intelligence to the member who submits it; and prevent the free-rider problem
Trusted Computing Group (Trusted Computing Group, https://trustedcomputinggroup.org/)	Trusted Computing Group	77	Protection of business-critical data and systems, secure authentication and strong protection of user identities, and the establishment of strong machine identity and network integrity
Cybersecurity Tech Accord (Cybersecurity Tech Accord, https://cybertechaccord.org/)	Microsoft	Over 150	Strong defense; no offense; capacity building; collective response
Global Cyber Alliance (Global Cyber Alliance, https://www.globalcyberalliance.org/)	New York County	186	Unite global communities; implement concrete solutions; and measuring the effect

implications, social meaning, and safety risks of the products and services. Even when people do not yet accept the social meaning of those products, let alone technical risk, they start using them because of convenience and because reliable data on product safety is so scarce that they often cannot make informed decisions. Even before the new products become normalized, they are pushed into the commercial market to make themselves subject to the systematic abuse of hackers and APTs. Some of the nonstate actors are malicious enough to use the products in highly harmful ways. One of the increasingly common ways for hackers to spread malware or finance covert actions is by mining and stealing cryptocurrencies like blockchain. To show the magnitude of compromised cryptocurrencies, the cybersecurity firm Optiv Security noted that in 2018, hackers delivered cyberattacks on systems like Litecoin Cash and MonaCoin at the rate of 51%. The 51% rate sounds like a hit or miss, but it is actually high by the industry standard, and the payoff is large; by 2018, hackers had stolen more than $800 million from such exchanges [37].

Another reason why norms fail to prevent attacks by nonstate actors is that, contrary to public statements, states have an inherent interest in keeping some distance from them. The term "distance" is used as a rhetorical expression here but has substantive implications. That is, the "closer" states' distance becomes to proxies, the more likely they are to be exposed when the proxies get caught. For example, over the years, the Italian cybersecurity firm Hacking Team has proliferated surveillance and decryption tools, communication monitoring devices, and systems that can remotely and secretly activate cameras. In 2015, hackers breached Hacking Team to reveal that it did business with governments in Sudan, Kazakhstan, and Bahrain, a corporate secret [37]. Close ties between government and firms were obviously the cause of the revelation. Moreover, close ties between government and nonstate groups can increase the likelihood of corporate fraud and corruption and consequently drive up prices for services and items the firms sell [38]. Therefore, states are naturally inclined to try to keep distance. However, if states operate too "far" from proxies, that causes different kinds of problems. That is, the proxies may become more likely to act independently of states. Some may feel so independent that they begin to disobey orders and falsely claim credit for actions they never took. Behavioral concerns like these force governments to spend extra resources to monitor the proxies and keep them from shaping policy preferences [39]. The proxies and firms may in turn refuse government monitoring to protect corporate and client interests [40]. This dilemma indicates that states have little control over firms' business decisions or little knowledge about for whom the firms ultimately work. This constitutes the other mechanism by which the current system allows nonstate actors to act at will.

In sum, the fact that international law and its many principles fail to incorporate the role of non-state actors into the preventive mechanism is critical. They have allowed threat groups and hackers to ignore their prescriptions and exploit technologies made by financially driven corporations to continue attacks on states. Large firms believe that they deserve a prominent role in generating peaceful norms when their normative output has not always been consistent with that of states. Furthermore, firms display a collective preference for defying the primacy of nation-states in favor of keeping operational flexibility and spurn the centrality of governments' roles in cyberspace regulations. The unaligned growth of firms' influence has undermined existing norms.

States' challenges with international norms

The other obstacle to efforts to prevent nonstate OCO is the disagreement between states. In particular, policy differences over what to do with cyberattacks are stark between Western states, Russia, and China. To be sure, they do agree over broad matters, such as the need to build international instruments to regulate cyberspace activities. As strange as it may sound, Russia has stressed the supremacy of international law in cyberspace and the desire to discourage competitors from exploiting vulnerabilities [23]. Of course, law is only "supreme" when it works for Moscow, and "competitors" happen to be whoever it is against. Some scholars claim that China shares with Western democracies a general commitment to the rule of law as a powerful force of convergence that will lead to overcoming points of contention. Zhixiong Huang and Kubo Mačák write, for example, "China and the West are slowly

coming together on many central issues, including Internet governance or sovereignty in cyberspace" [41].

Obviously, the devil is in the detail. Russia and China have promoted a state-controlled approach to cyber-sovereignty, a notion that governments have exclusive power of jurisdiction over national cyberspace, when Western democracies support a decentralized form of internet governance. Their strategic thought has much to do with the type of political environment they operate relative to their rivals. They reject the current rule-based liberal world order, which they perceive as a firm indicator of Western imperialism and a threat to the way they govern. Russia and China uphold the principle of nonintervention into internal affairs (except for their adversaries') and seek to use international legal frameworks to enhance the principle of self-determination. They openly reject foreign propaganda, influence campaigns, and what they perceive to be Western attempts at regime change, except when they serve their interest. They see online freedom and unregulated information flow as a primary risk to domestic order and seek to achieve "information security" more than cybersecurity.

The most heated battleground of cyber norms is at the United Nations. The history of contestation is relatively short, but it is long enough to have witnessed the failure of global discourse to prevent cyber attacks, including those launched by nonstate actors. It started in 1998 when Russia demanded a multilateral treaty to regulate the use of ICTs in international conflict before Western states declined to negotiate it in favor of standing international law. The first GGE ran its program through 2005 when the international community focused much of its attention on global terrorism and the Iraq war of 2003, but the second GGE reached global consensus in 2010 on the need to focus on emerging threats. In 2013, the third GGE recognized that international law is applicable in cyberspace. In 2017, we saw the GGE "collapse" when it failed to punch out substantive outcomes in its report, prompting observers to declare the end of cyberspace norms. The collapse served as a brutal reminder of the difficulty of working through international institutions.

The end, if any, was short-lived because in 2018, UN Member States rebounded from the 2017 debacle to rekindle the hope for an institutional solution. But the revival underscored the contested nature of discourse. Member States passed resolutions in the General Assembly to produce not one but two parallel processes. On the one hand, the US resurrected the GGE to get its participants to press others to stop peacetime targeting of critical infrastructure, political interference, and theft of intellectual property and to penalize perpetrators. This GGE reports to the 76th GA session in 2021 to clarify how international law applies to cyberspace. As before, GGE membership includes the 5 permanent members of the Security Council and 10 other states chosen by grouping. On the other hand, Russia created the Open-Ended Working Group (OEWG), an alternative norm-making forum whose membership is open to all UN member states, unlike GGE. OEWG has a broader set of areas to explore than GGE – existing and potential threats, international law, rules, norms, and principles, regular open-ended dialog, CBM, and capacity building. Note that these norms are so repetitive and elementary in substance that they appear to be foot-dragging efforts, as if nations have wasted all these years only to get this far. What is important, however, is that the competition indicates a fractured norm process.

Of course, there are some positive aspects one can draw from the discourse. For one, cross-membership in GGE and OEWG enables greater information-sharing and trust-building. Both groups operate based on consensus, so expectations for substantive progress are naturally limited [42]. However, while the mandates of these two processes overlap significantly, membership is vastly different [43]. Conflicting membership makes discordance more apparent than coordination. In fact, existing fractures seem to have deepened as the latest GGE and OEWG rounds have operated based on *separate* meeting schedules at the average interval of every other week, with few overlaps. The division is so public that US Deputy Secretary of State John Sullivan (2017–present) acknowledges that OEWG may hamper GGE progress and harm established norms [1].

Conclusion

This article exposes at least two ironies, one regarding international law and the other about cyberspace norms. The first irony is that international law has promoted state centrism for so many years that, once in the cyber age, the very legal foundation that is supposed to protect states has become the major obstacle to promoting state security. The other irony is about norm politics; major powers in cybersecurity – especially the USA, Russia, and China, each of which have promoted norms – have been among the greatest violators. This article suggests that all kinds of moral charges can be made about embedded hypocrisy and the double standard of words and deeds. Worse, these powerful states are not just violating each other's norms but creating a strategic environment that permits norm contestation and overlooks further violations, including those committed by nonstate actors. The hypocrisies, however, precisely underscore the true state of cybersecurity where power and interest forge around powerful states, and there is limited space for international law and norms to play a larger role in regulating their behavior.

This article indicates the need for the reconsideration of state commitment to the existing international legal and norm system as a preventive mechanism against nonstate OCO. Space limitation precludes further discussions of specific policies on international law and norms beyond the ones that I presented above. This analysis, however, provides a sufficient narrative that reform is necessary for the international system to be effective against nonstate OCO. It is apparent that cyberspace norms – especially principles like those of distinction, due diligence, and proportionality – must be updated to reflect the growing influence of nonstate actors in cyberspace. At the same time, it remains true that states have sought to reform the system and make norms robust over the years without achieving meaningful change. Rather than promoting international law and norms as a means of preventing cyberattacks, states and private actors are likely to depend more on themselves to prevent nonstate attacks. For one, scholars have called for a variety of active defense countermeasures to be adopted. A reasonable action we can expect states to take is the consideration of how international law and norms can aid state conduct of active defense in cyberspace. In this context, what is required is a series of examinations regarding what specific aspects of international law ought to be reformed and which one of the many ideas and principles can be facilitated to generate more effects than before.

Acknowledgments

The author presented earlier versions of the paper at Oxford University, Saint Louis University, and Washington University in St Louis and thanks the audience for providing feedback. The author also thanks Timothy Lomperis, Joseph Scherrer, and Andrew Sobel for their comments, Julia Gerwe, Emily Johansson, and Margaret Kenney for superb research assistance, and the three reviewers of this article for excellent suggestions. Finally, I thank Saint Louis University for financial support.

References

1. Ravie L. Hackers created thousands of coronavirus (COVID-19) related sites as bait (March 18, 2020), The Hacker News. https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html; World Powers are Pushing to Build their Own Brand of Cyber Norms. CYBERSCOOP (September 23, 2019).
2. Hackers created thousands of coronavirus (COVID-19) related sites as bait (March 18, 2020), The Hacker News.
3. Nye J. Deterrence and dissuasion in cyberspace. *Int Security* 2016/2017; **41**:60.
4. Lin H. Offensive cyber operations and the use of force. *J Natl Security Law Policy* 2010;**4**:63.
5. Donno D. *Defending Democratic Norms: International Actors and the Politics of Electoral Misconduct*. Oxford: Oxford University Press, 2013.
6. Delerue F. *Cyber Operations and International Law*. Cambridge: Cambridge University Press, 2020.
7. Dinniss H. *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, 2012, 233.
8. Mačák K. From cyber norms to cyber rules: re-engaging states as law-makers. *Leiden J Int Law* 2017;**30**:877–899.
9. Mačák K. *Internationalized Armed Conflicts in International Law*. Oxford: Oxford University Press, 2018.
10. Schmitt M. *Tallinn manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, 156.
11. Schmitt M, Watts S. Beyond state-centrism: international law and non-state actors in cyberspace. *J Conflict Security Law* 2016;**21**:595–611.
12. Efrony D, Shany Y. A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice. *Am J Int Law* 2018;**112**:583–657.
13. d'Aspremont J. Cyber operations and international law: an interventionist legal thought. *J Conflict Security Law* 2016;**21**:575–593.
14. Schmitt M. *France's Major Statement on International Law and Cyber*. New York, NY: Just Security, New York University School of Law, 2019.
15. Broeders D, De Bussar E, Pawlak P. *Three tales of attribution in cyberspace: Criminal law, International Law and Policy Debates*, 2020 Policy brief. The Hague Program for Cyber Norms, April 2020), 6.
16. Ahmad A, Webb J, Desouza K, Boorman J. Strategicallymotivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Comput Security* 2019;**86**:407.
17. Finnemore M, Hollis D. Constructing norms for global cybersecurity. *Am J Int Law* 2016;**110**:425–479.
18. Nye J. Normative restraints on cyber conflict.*Cyber Security*, Vol. **1**. London, UK: Henry Stewart Publications, 2018, 11.
19. McKune S. "Foreign Hostile Forces" The Human Rights Dimensions of China's Cyber Campaigns. In: Lindsay JR, Cheung TM, Reveron DS (eds.), *China and Cybersecurity*. Oxford: Oxford University Press, 2015.
20. Chaudhary T, Jordan J, Salomone M *et al.* Patchwork of confusion: the cybersecurity coordination problem. *J Cybersecurity* 2018;**4**.
21. Geers K. *Strategic Cyber Security*. Tallinn, Estonia: CCD COE Publication, 2011, 116.
22. Hathaway O, Crootof R, Levitz P *et al.* The law of cyber-attack. *California Law Rev* 2011;**100**:873.
23. Giles K, Monaghan A. *Legality and Cyberspace*. Carlisle, PA: USAWC Strategic Studies Institute, 2014, 19.
24. Fischerkeller M, Harknett R. Deterrence is not a credible strategy for cyberspace. *Orbis* 2017;**61**:381–393.
25. Kello L. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press, 2017.
26. Valeriano B, Ryan M. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press, 2015.
27. Finnemore M, Sikkink K. International norm dynamics and political change. *Int Org* 1998;**52**:887–917.
28. Nye J. *Eight Norms for Stability in Cyberspace*. The Hague, The Netherlands: The Secretariat of the GCSC, 2019.
29. Google Security Blog, Vulnerability Reward Program: 2019 Year in Review (January 28, 2020).
30. Schmitt M. Grey Zones in the International Law of Cyberspace. *Yale J Int Law* 2017;**42**.
31. Schmitt M. Below the threshold' cyber operations: the countermeasures response option and international law. *Virginia J Int Law* 2014;**54**: 704–705.
32. Chertoff M. *Exploding Data: Reclaiming Our Cyber Security in the Digital Age*. New York: Grove Press, 2018.
33. Fischerkeller M. Incorporating offensive cyber operations into conventional deterrence strategies. *Survival* 2017;**59**:103–134.
34. Farrell H, Charles G. How effects, saliences, and norms should influence U.S. Cyberwar Doctrine. In: Lin, HZegart A (eds.), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington, DC: Brookings Institution Press, 2019, 58–60.
35. Small Contractors Struggle to Meet Cyber Security Standards, Pentagon Finds Defense One. (December 2, 2019).
36. Dobrygowski D. Why companies are forming cybersecurity alliances. *Harvard Business Review* (September 11, 2019).
37. Optiv Security. 2019 Cyber Threat Intelligence Estimate, Denver, 2019.
38. Lachow I, Grossman T. Cyberwar Inc.: examining the role of companies in offensive cyber operations. In: Lin, HZegart A (eds.), *Bytes, Bombs, and Spies*. Washington, DC: Brookings Institution Press, 2019, 390–391.
39. Maurer T. Cyber proxies and their implications for liberal democracies. *Washington Q* 2018;**41**:171–188.
40. Kello L, Private sector cyber weapons: an adequate response to the sovereignty gap? In: Lin, HZegart A (eds.), *Bytes, Bombs, and Spies*. Washington, DC: Brookings Institution Press, 2019, 357–378.
41. Huang Z, Mačák K. Towards the international rule of law in cyberspace: contrasting chinese and western approaches. *Chin J Int Law* 2017;**16**: 271–310.
42. Korzak L. What's Ahead in the Cyber Norms Debate? Lawfare 2020. https://www.lawfareblog.com/whats-ahead-cyber-norms-debate (March 16, 2020).
43. Broeders D, Cristiano F. Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road. *Italian Institute for International Political Studies* (April 2, 2020).