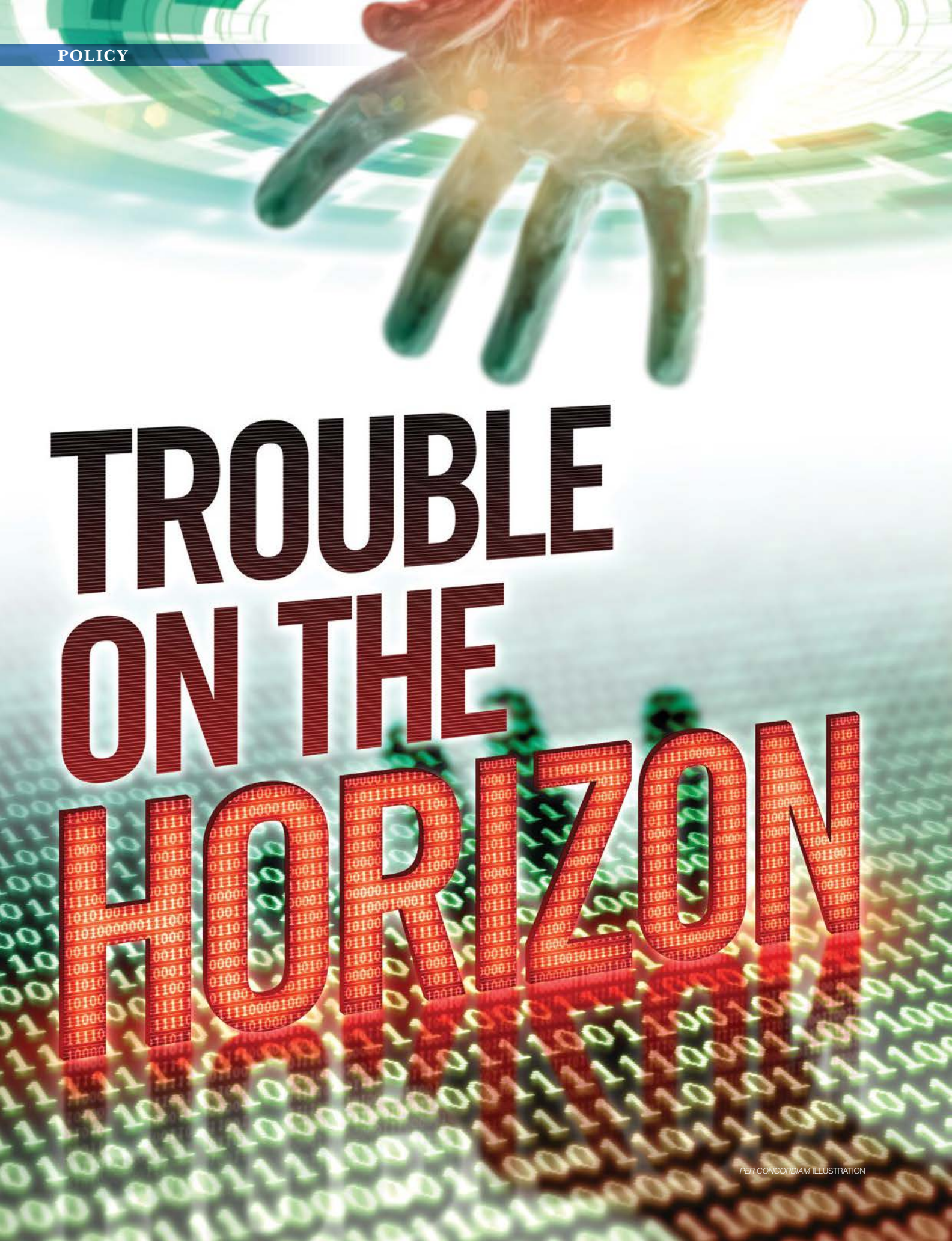

PER CONCORDIAM ILLUSTRATION

A looming cyber warfare threat demands an overhaul of international law

By Lt. Col. Brian Smith, U.S. Central Command

PHOTOS BY THE ASSOCIATED PRESS

Although some progress has been made over the past decade, current international law governing cyber warfare remains vastly inadequate. It is rife with ambiguity, fails to provide legal grounds for proportional retaliation in catastrophic scenarios, and fosters an international environment in which states feel no compulsion to treat cyber warfare as "warfare." As Sean D. Murphy notes in his 2012 book *Principles of International Law*, since the creation of Article 2(4) of the United Nations Charter, the International Court of Justice (ICJ), politicians and international law scholars have grappled with determining what exactly constitutes "use of force" and, therefore, what constitutes *jus ad bellum* (right to war). Also, the meaning of the term "use of force" is debatable; the U.N. General Assembly's 1974 resolution defining aggression failed to address many of the types of actions that might be deemed unlawful uses of force. Furthermore, what constitutes the right of self-defense, as outlined in the U.N.'s Article 51, has likewise been highly debated.

With the rapid increase in hacking in recent years, the need to address cyber warfare in explicit detail remains urgent. The failure to do so will eventually become catastrophic. In his 2014 book *Cybercrime and Cyberwarfare*, Igor Bernik finds that cyber warfare unfortunately fails to garner the attention it deserves within the international community. The U.N., NATO and other international organizations have faced cyber attacks on numerous occasions over the past decade, as noted by Nils Melzer in a 2011 paper, "Cyberwarfare and International Law." But none of the incidents led to significant change in international law, primarily because none of the incidents led to tragedy. That would change, however, with an attack resulting in a large number of casualties and billions in property damage.

Legal ambiguities

Cyber warfare is quickly becoming one of the leading global threats to industrialized nations. Yet the international law surrounding the threat remains rife with ambiguity. According to Murphy, at the center of this ambiguity are three critical questions. First, does a cyber attack constitute a use of force in violation of Article 2(4)? Second, does Article 51 allow a state to engage in cyber warfare pre-emptively? Third, should nonstate actors who conduct cyber warfare be treated the same as state actors? Sadly, investigations and legal maneuvers in the wake of cyber attacks in recent years have done little to address the ambiguity.

Although deliberations by the U.N. General Assembly and subsequent rulings by the ICJ support the conclusion that a cyber attack constitutes a use of force in violation of Article 2(4), this conclusion still comes with a degree of ambiguity. The General Assembly's 1974 "Definition of Aggression," published in Resolution 3314, defines aggression as the "use of armed force by a State" and provides a list of acts that qualify as aggression. In six of the seven acts, the term "armed forces" is reiterated, thus reinforcing its importance. Unfortunately, the term itself is not well-defined and the list of acts provided is remarkably small. Furthermore, in the first act listed, an "attack by the armed forces of a State," the word "attack" is not defined, according to Steven R. Ratner in his 2002 paper in the *American Journal of International Law*. Adding to the ambiguity, the Definition of Aggression also states that the list of acts is not exhaustive and that the U.N. Security Council may add to it.

Ratner also states that, despite the lack of clarity, Resolution 3314 confirms the understanding that aggression includes a variety of acts, and ICJ cases decided since the Definition of Aggression was published conclude that cyber attacks constitute a use of force. In the 1986 decision Nicaragua v. United States, the ICJ stated that sending armed bands amounts to an armed attack only if "because of its scale and effects" it serves as something more than a "mere frontier incident." This decision afforded states the opportunity to declare other states as aggressors even when the actions in question clearly fail to fall within the purview of the Definition of Aggression. As J. Martin Rochester noted in his 2006 book, *Between Peril and Promise: The Politics of International Law*, interstate war, particularly over territory, has become a "relatively peripheral concern" and remarkably infrequent. However, this uplifting fact is offset by the

reality that acts and threats of violence remain prevalent across the world, only in more complex forms more difficult to legally grasp. Rochester further states that the decline of interstate war as a ubiquitous norm of international relations has given way to what the Prussian military theorist Carl Von Clausewitz called "war by other means." The ability of international law to specifically label new forms of aggression as such is becoming more tenuous with each passing decade. The rapid evolution of cyber warfare, and whether a cyber attack constitutes a use of force in violation of Article 2(4), must be properly addressed if international laws governing cyber warfare are to advance and provide adequate legal recourse to victims.

Perhaps even more ambiguous than Article 2(4) and the use of force, is whether Article 51 allows a state to engage in cyber warfare pre-emptively, a question hotly debated in the international community. Marco Roscini, in his 2014 book, *Cyber Operations and the Use of Force in International Law*, argues that under Article 51, a state targeted by a cyber operation may only claim self-defense and react forcibly if the operation amounts to an "armed attack." He further notes that such an attack applies not only to traditional weapons, but also to "one with cyber means," provided that the extent of the attack amounts to a use of force under Article 2(4). This was reinforced by the 2004 opinion of the U.N.'s High-Level Panel on Threats, Challenges and Change, which appeared to support the loosening of the strict prerequisite of an "armed attack" as the only justification for a forcible reaction, according to a 2006 article by W. Michael Reisman and Andrea Armstrong in the *American Journal of International Law*. Providing a contrary opinion, Reisman and Armstrong argue that whether wise or not, Article 51 was not written to accommodate even the Caroline principle, considered by many international law scholars to be the standard for establishing a pre-emptive self-defense claim of any kind. Furthermore, they point out that in a series of judgments and advisory opinions, the ICJ held firmly to a strict reading of Article 51, concluding that a state's right to claim self-defense is subject to it "having been the victim of an armed attack."

Regarding the third question at the center of cyber law ambiguity — should nonstate actors who conduct cyber warfare be treated the same as state actors? — the U.N. Charter once again fails to provide clear legislation for the domain of cyber warfare. Richard A. Clarke and Robert K. Knake, in their 2010 book *Cyber War: The Next Threat to National Security and What to Do About It*, define cyber warfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." Their use of the term "nation-state" undoubtedly stems from the recurring use of the word "state" within Resolution 3314. As Bernik also finds, the lack of specific universal definitions and the lack of consensus on the definition of key concepts alone indicates that cyber criminals continue to stay ahead in the fight. The continued use of the word "state" in Article 2(4) and the failure of international law to distinguish properly between the actions of state and nonstate actors adds to the ambiguity of cyber warfare. This failure turns the debate into a war of semantics, similar to the debate surrounding the invasion of Iraq in 2003. As Curtis A. Bradley and Jack L. Goldsmith noted in their 2005 *Harvard Law Review* article, many times prior to 2003, U.S. presidents initiated hostilities without congressional authorization, even when, arguably, in violation of the U.N. Charter.

Shaky legal ground

Current international law fails to prevent or discourage the use of force within the cyber domain because it fails to provide legal grounds for proportional retaliation in catastrophic scenarios. In a world increasingly dominated by cyberspace, the need for appropriate cyber warfare legislation is becoming more urgent. Unfortunately, as Jack L. Goldsmith and Eric A. Posner remark in a 1999 University of Chicago Law School article, *opinio juris*, legality, morality and similar concepts mean little to states on the international stage, and one could argue that they mean much less to the primary actors of the cyber domain. Most cyber actors will never comply with the norms of international law out of a sense a moral or legal obligation. They will comply when it's in their own states' interests. Further, Jason D. Jolley writes in his paper, published in the Canadian Center of Science and Education journal *International Law Research* in 2013, that without adequate legislation prohibiting cyber warfare, states will continue to disregard international norms and utilize their technological expertise to unleash cyber attacks. As long as states can argue that their actions do not violate international law, they will continue to exploit other states' weaknesses for economic, political or military advantage, resulting in a continuous escalation of nefarious acts to the point where large-scale tragedy becomes inevitable.

To understand the seriousness of cyber warfare and the inadequacy of international cyber warfare legislation, one must take a hard look at what cyber actors are capable of and the legal options available to their potential victims. Clarke and Knake warn that cyber attacks have the potential to cause airplanes to crash, trains to derail, chemical plants to release poisonous gas, gas pipelines to explode, enemy units to walk into ambushes and much more. In this doomsday scenario, a sophisticated cyber attack on America's infrastructure cripples the most advanced nation on the planet in a mere 15 minutes and causes the deaths of thousands of people. Such a massive and coordinated attack seems highly implausible, but to test the limits of current cyber warfare legislation, one need only consider the consequences of just one of these tragic events.

One scenario involves hackers infiltrating a nuclear power plant and causing a power surge, which triggers an attempted emergency shutdown, a much larger subsequent spike in power output and eventually a reactor vessel rupture. Following the rupture, a series of steam explosions exposes the internal structure of the reactor to air, causing it to ignite. The resulting fire sends radioactive fallout into the atmosphere, which then lands and contaminates millions of acres and those living on it. The immediate death toll is in the dozens, but the expected long-term death toll reaches the thousands. As unlikely as the scenario may sound, the two critical events

German Interior Minister Thomas de Maiziere stands before a map in February 2017 that illustrates the number of cyber attacks in Europe over a 30-day period.

of this scenario have already played out in real-world events, according to Jolley. In 2010, a malicious software virus named "Stuxnet" caused as many as 2,000 centrifuges at an Iranian nuclear power plant to change speeds rapidly, inducing vibrations that destroyed the centrifuges. In 1986, the Chernobyl Nuclear Power Plant suffered an unexpected power surge that resulted in radioactive fallout.

There is nothing preventing a virus like Stuxnet from being used to cause the type of accident that occurred in Chernobyl. And when an event of this magnitude eventually does take place, according to Paul Rosenzweig's 2013 book *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, the international community will undoubtedly realize that existing international legislation fails to address such an attack. In addition, long-standing assumptions and frameworks for settling conflict will disappear, seemingly overnight, and how states fight wars will have to be rethought, as will the definitions of armed attack, terrorism, espionage and crime. The atomic bombings of Hiroshima and Nagasaki were the last time the international community was forced to examine the limits of international law so carefully. Although Stuxnet caused nowhere near the same level of destruction, Rosenzweig writes that the "cognitive disruptions that will come are just as great" and that the virus was, figuratively, just the first explosion of a cyber atomic bomb.

When investigating the future of cyber warfare and the potential devastation that lies ahead, Jolley reminds us it is critical to remember how electronically interconnected states are and how much cyberspace dominates the world. An enormous portion of our lives is controlled by computer systems and networks, from utilities to shopping and from banking to social interactions. Critical infrastructure depends almost completely on computer systems and networks to control everything from commercial transportation to water purification, to communications and much more. Because of our dependence on cyberspace, Jolley states, we must re-evaluate the definition of the "use of force" and how to test for it. In short, the international community must rewrite the rules of cyber warfare and establish a multilateral treaty prohibiting the "use of force" in the cyber domain.

International indifference

Despite large-scale cyber attacks over the past decade, the international community continues to muddle along without legislation capable of dealing with cyber warfare. As Bernik remarked, "outdated, rigid, and fragmented legislation"

A French police officer works at a state-sponsored facility that investigates cyber crimes reported by the public.

prevents the development of physical and legal safeguards to cyber warfare by competent authorities and prevents the proper courses of action being taken by victims of cyber attacks. At the heart of the issue lies a pervasive mood of general indifference, which owes its existence to a variety of more specific issues. First, the international community's overall knowledge of the cyber warfare threat remains remarkably limited. Second, a viable approach for developing adequate cyber warfare legislation appears elusive. Third, even if adequate legislation did exist, the perpetrators of cyber warfare display far less respect for international law than those fighting against them, making compliance difficult to achieve. Unlike the typical actors in past interstate wars who held at least some regard for their standing within the international community, today's typical cyber warrior is often nothing more than a small terrorist or political organization with no concern for international law. The lack of knowledge can and almost certainly will be fixed over time, if only in the aftermath of tragedy; however, the demographics surrounding cyber warfare make the third issue far more problematic than the first two.

Improving cyber warfare legislation won't happen until the international community fully understands the threat. Fortunately, as Stephen D. Krasner notes in his 1982 article in the journal *International Organization*, history shows that increased knowledge plays an invaluable role in revolutionizing politics and states' behavior, especially in areas such as public health and arms control. For example, the explosion of global scientific knowledge in the mid-20th century radically altered rules governing the use of vaccines. Prior to the explosion, national health regulations regarding vaccines were dictated by politicians with no medical knowledge, but afterward national policies were influenced by an international regime. The same held true with the arms race. The realization of mutual assured destruction (MAD) by both the U.S. and the Soviet Union provided a basis for a regime. Without both sides knowing the reality of MAD, knowledge would have had no impact on regime development. Ironically, cyber warfare appears to be developing into a new type of arms race and, hopefully, the international community will respond with appropriate legislation before tragic events unfold.

In addition to the lack of awareness of the cyber warfare threat, the international community also lacks a viable approach for developing adequate legislation. On opposing sides of the fight are realists, who believe that institutions play a minimalist role in influencing state behavior, and liberal institutionalists, who believe that institutions are the key to influencing state behavior. In his 1994 article, "The False Promise of International Institutions," John J. Mearsheimer argued that the international system is anarchic and institutions are little more than a reflection of the balance of power in the world. He further remarked that many policymakers naively believe that institutions hold great promise for creating international peace. Considering the present anarchic nature of the cyber world, where actors operate largely in the shadows and their actions are difficult to trace and nearly impossible to prosecute, Mearsheimer's view appears to hold water in cyberspace. At all levels, cyber actors "look for opportunities to take advantage of each other," and at the state level actors strive not only to achieve cyber hegemony but also to prevent other actors from achieving the same lofty position. An offensive realist such as Mearsheimer would likely argue that a powerful state actor in the cyber domain would be wise to attempt to achieve hegemonic status before others do, especially considering that if executed properly, such a status could be achieved before the rest of the actors even realized it. Nevertheless, from the present and impersonal state of the cyber domain, it is easy to see why many actors feel frustrated by the failure of institutions to achieve peace and order and, hence, why indifference runs rampant.

Taking a more optimistic approach, institutionalists argue that it is not necessary to develop cyber warfare legislation under the backdrop of a doomsday scenario, such as that proposed by Clarke and Knake, and that the vast majority of international laws exist to control state behavior in very benign circumstances. Despite the widespread opinion of cyber experts that it's only a matter of time before a large-scale cyber attack takes place with tragic consequences, few believe that cyber warfare is an existential issue for states. In 2004, Detlev F. Vagts analyzed the Goldsmith-Posner view on customary law and noted in his essay in the *European Journal of International Law* that customary law is strongest when "the

costs of compliance are not enormous." By this, Vagts simply implies that there are many laws that don't directly deal with the life and death of the state, and those laws are important, too. Cyber laws will become more critical to the international community with every passing year, but they will never be about state survival. With this in mind, it is important to realize that some success in cyber legislation is better than no success at all. Myres S. McDougal, in the 1952 article "Law and Power," wisely notes that people who truly strive to avoid violence, except in self-defense or organized community sanction, have only the alternative of some type of law, whether domestic or international. This is especially true of countries incapable of defending themselves against much more powerful belligerents. He continues by arguing that the choice cannot be between law and no law, but rather between effective and ineffective law. John Gerard Ruggie summarized the realist approach in his 1995 paper, "The False Premise of Realism." Noting that, however weak institutions might be today, even minimal contributions of peacekeeping and nonproliferation are better than nothing.

Perhaps the greatest cause of indifference and, simultaneously, the greatest threat to any future cyber warfare legislation is the perceived potential of noncompliance. Given the extraordinary nature of cyber warfare and the rate of its evolution, past theories on why states obey international law may not apply to this domain. In their 2012 paper, "Constructivism and International Law," Jutta Brunnée and Stephen J. Toope argue that law becomes persuasive when the relevant actors view it as legitimate, especially when it inspires reasoned argument to justify its processes. This view is supported by Thomas M. Franck in a 1988 article in the *American Journal of International Law*, but he adds that "in a community organized around rules, compliance is secured — to whatever degree it is — at least in part by perception of a rule." Here, Franck implies that legitimacy of legislation as a solution for state compliance is only guaranteed to be applicable in a community that already respects rules. For terrorist organizations or states that sponsor or support terrorism, such as North Korea and Iran, legitimacy of cyber warfare legislation means almost nothing because such entities have little or no respect for rules or regimes. Furthermore, the Franck fairness model holds little promise for compliance in a domain where it is difficult to obtain the evidence needed to prosecute violations of law.

Adding to the potential for noncompliance, the cyber warfare domain does not benefit from standard constructivist tools that further the development of international law in other domains. As Brunnée and Toope noted, actors "learn" through patterns of interaction to read the social environment in which norms are shaped and influenced. Unfortunately, the primary actors in the cyber domain, or at least those that "first world" states are most concerned about, are typically actors who have little or no meaningful interaction with those that they target. Cyber criminals, from the lone hacker in a basement to a state-sponsored group in China, do not socially interact with others on an international stage or in ways that foster the development of appropriate cyber law. Furthermore, as Brunnée and Toope argue, the social interaction needed to further the development of cyber law is only effective when most of the actors involved believe that most others will understand the laws the same way they do and comply in the same way. Such would not be the case in the cyber domain.

Leading theorists of international law provide a wide variety of reasons for the international community's indifference to cyber warfare law. Ultimately, as Harold Koh noted in his 1997 article "Why Do Nations Obey International Law?" no one theory can explain the behavior of all states all of the time, and thus, the only way to determine what will make cyber warfare actors comply is a thorough analysis of all reasonable theories, drawing from them the characteristics that appear most applicable.

Conclusion

The world has not yet witnessed dramatic humanitarian consequences as a result of cyber warfare but, as Melzer points out, the potential for human tragedy is enormous and increases every year as our lives become more and more dependent on computer-controlled systems. As far as international law is concerned, cyber warfare does not exist in a vacuum, but it has not been given the attention it deserves. To deter large-scale cyber attacks and prevent smaller attacks from escalating into larger ones, the international community must begin to transpose existing rules and principles to the relatively new domain of cyber warfare. New treaties must be forged and existing definitions must be changed. Doing so will be difficult because the international community is largely uneducated in cyber warfare, the technologies within the cyber domain change so rapidly, and many of the key actors in the domain are unidentifiable and uninterested in changing the rules.

From a theoretical standpoint, it is difficult to gauge whether new international laws will see greater success from a realist or institutionalist perspective. Realists focus primarily on the international-system level of analysis and dismiss the importance or impact of the individual and the nature of the state in the decision-making process. Therefore, realists and neorealists such as Mearsheimer would likely argue to leave institutions such as the U.N. and NATO out of the picture. Such a perspective is convenient for citizens of the most powerful state in the world, but it wouldn't sit well with smaller states, such as Estonia, which depends on international institutions for protection and in 2007 suffered the largest cyber attack to date at the hands of neighboring Russia. On the other hand, realists consider states to be a group of introverts incapable of rational dialogue and suspicious of every foreign move, and such a description is very applicable to many of the primary actors in cyber warfare. Regardless, due to the uncertainty that lies ahead in the cyber domain, some action is better than no action at all and it is time for the international community to rewrite the rules of cyber warfare. As the Dutch jurist Hugo Grotius brilliantly remarked, "All things are uncertain the moment men depart from law." □