
Jon P. Jurich

Follow this and additional works at: https://chicagounbound.uchicago.edu/cjil

Recommended Citation
Available at: https://chicagounbound.uchicago.edu/cjil/vol9/iss1/11

This Article is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in Chicago Journal of International Law by an authorized editor of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.
I. INTRODUCTION

After Estonia relocated a Soviet World War II memorial in late April 2007, the country fell prey to a series of distributed attacks which suddenly jammed and disabled various websites by overcrowding the bandwidths for the servers running the sites.\(^1\) Among the servers targeted were those hosting the websites of the Estonian president, major Estonian news agencies, government ministries, and two of the country's largest banks.\(^2\) Attempts to trace some early attacks revealed that at least some of the attacks had Russian origins and were alleged to have emanated from Russian state institutions.\(^3\) The attacks seemed to pour in from around the globe, however, making Estonian assertions of culpability hard to prove.\(^4\)

"Cyberwarfare," as these attacks were described, represents the emerging use of the internet to disrupt national security as cyberspace has become better developed and increasingly accessible to all parts of the world. The breadth of the attacks against Estonia, however, highlights the scope of modern technological vulnerability: attacked websites included a broad range of

---

\(^1\) Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, Guardian HP1 ¶ 19 (May 17, 2007), available online at <http://www.guardian.co.uk/russia/article/0,2081438,00.html> (visited Apr 5, 2008). Such attacks are commonly known as distributed denial of service attacks and are characterized by overt attempts to deny services to their legitimate users. Id at ¶ 18.

\(^2\) Id at ¶ 14.

\(^3\) Id at ¶ 19.

\(^4\) Id.
important networks affecting government, civil information, and financial markets, all institutions which underpin modern life.

The global community's increasing reliance on information technologies has highlighted the need for governing laws for these new and evolving technologies that are being adopted at an increasingly rapid pace. Such law, however, has come in fits and starts, limited by a lack of universal accord governing these technologies, a disparity in national regulations, and questions of national sovereignty.

At the same time, commentators have called into question the longstanding traditional view that customary international law is formed exclusively by states' acts and beliefs. The challenge to this traditional understanding, which includes an attack on the consensualist conception of international law, suggests a potential alternative framework by which to structure an international law governing cyberwar. This Development undertakes an analysis of this realist perspective on customary international law formation and highlights the advantages and disadvantages that relate to its application to the issue of an international law governing cyberwar.

Section II of this Development explores the various definitions of cyberwar, information operations, information warfare, and cybercrime. This exploration attempts to create a stable ground that accounts for widening dependence on network technologies, the challenges in separating their military and nonmilitary uses, and the threats and opportunities which result from their use. Section III examines how current law governs the use of these technologies and identifies the areas in which existing law struggles to meet the challenges of the emerging technologies and their users. Section IV analyzes the realist perspective of customary international law and its reflections in developing international law and considers the possibility that a nonstate-based governing law of cyberwar could emerge.

II. INFORMATION OPERATIONS, INFORMATION WARFARE, AND CYBERCRIME

Analyzing cyberwar requires defining the relevant terminology. Broadly defined, information operations ("IO") includes offensive and defensive actions that attack or protect information systems. Information systems here include

6 See id at 159.
the infrastructure, components, organizations, and personnel that deal with information. The inclusion of infrastructure and personnel makes the IO definition overly broad when developing an international law for actions solely within the networked world. Attacks against or damage to the infrastructure and its personnel can largely be addressed by existing laws, as those laws already prevent actors from committing crimes against property. A new law only needs to address a narrower portion of information operations.

The US Air Force definition of information warfare ("IW"), concentrated on the denial, exploitation, corruption, and destruction of information within information systems (or on preventing such an event), helps limit the scope of the inquiry. This definition focuses on the types of attacks that alter information within the system but do not visibly change the physical entities which provide the information (such as a server). This definition does not limit the physical effects which could occur outside of the information system as a result of the attack, but distinguishes neatly between the types of attack already governed by existing laws and this new, more concerning variety. To illustrate, the destruction of a computer or its hard drive is governed by an easily applicable law; the alteration of the contents of its hard drive, or of its ability to access a larger network without actually damaging the physical components of the computer, poses a more difficult question. IW also has two subsets; one form of IW involves misinforming an opponent, while another, the computer

---

9 This point holds true particularly given the intertwining of military and nonmilitary uses that makes almost any information systems infrastructure part of the military. See US v Kabat, 797 F2d 580 (8th Cir 1986).
11 Id at 947 (quoting Office of the Judge Advocate General, Headquarters USAF, Primer on Legal Issues in Information Operations 14 (USAF, draft 3d ed, Oct 1997)). Note that this definition has narrower limits than the definition of computer network attacks, which are "[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Schmitt, 37 Colum J Transnatl L at 888 (cited in note 7) (quoting Joint Chiefs of Staff, Joint Pub 3-13, Joint Doctrine for Information Operations GL-5 (Oct 9, 1998)).
12 For example, a terrorist altering data in an air traffic control computer could produce significant physical consequences, but could do so without making any change to the physical equipment providing the controller with information.
network attack ("CNA"), more actively destroys or alters the opponent's information.

Even within the limited scope of attacks on information, cyberspace's many uses—and an increasing global reliance on the application of these uses—leaves myriad potential methods available to attackers. The intertwined nature of cyberspace's infrastructure places military, government, financial, and civilian uses into a single channel. Within this channel, technological breakthroughs create vulnerabilities for all users, who are open to opponents' exploitation. These opponents may range from economic, political, and military competitors to terrorists and criminals. Each technological breakthrough, moreover, opens all users of the infrastructure to attacks from any individual opponent. Meanwhile, opponents can develop offensive strategies against a variety of targets simultaneously because of a shared protocol within the infrastructure.

Despite this growing threat, leading nations continue to evolve toward a greater reliance on information systems. The Chinese government has committed itself to developing an "informationalized" army, comprised of individuals manning computer terminals instead of tanks, to replace current "mechanized" technology, and the US Department of Defense ("DOD") uses over two million computers and more than ten thousand local area networks, most of which are linked to, and vulnerable to attack from, users of the larger internet. The push towards greater reliance on information technologies in fields including energy, communications, industry, finance, transportation, and human services has produced a situation in which economic collapse could occur even if only the financial components of the information systems were crippled; a more widespread attack could lead to an even greater disaster.

In conjunction with a wide array of targets, the nature of the cybersphere creates a host of potential attackers. Some consensus exists that the world's

13 Schmitt, 37 Colum J Transnat'l L at 888 (cited in note 7).
15 Schmitt, 37 Colum J Transnat'l L at 887 (cited in note 7).
16 Id at 894–95.
17 Philip M. Romero, An Immunological Approach to Counter-Terrorism and Infrastructure Defense Law in Electronic Domains, 14 Intl J L & Info Tech 101, 103 (2006). Romero also notes that no clearer vulnerability can exist than the United States Federal Reserve going online. The Fed has decided to allow the nation's money supply to move almost entirely over the Internet. The old system for transferring US dollars safely, Fedwire, was a closed network that was not attached to the internet, moving about $1.8 trillion a day, and averaging $3.5 million per transaction. FedLine, the new system, is Internet based, and is expected to move even larger amounts.

Id at 128.
major powers are unlikely to engage in offensive direct conflicts with each other by either traditional means or IW. In a world with established military and economic disparities, however, emerging nations and nonstate actors that make traditional attempts to harm a dominant adversary will likely compete asymmetrically, making the use of IW more attractive to less well-heeled combatants. Estimates suggest that ten individuals with $10,000 could cause a several week-long disruption of the US defense information infrastructure, while one hundred individuals with $30,000,000 could so thoroughly corrupt the country’s entire information infrastructure that recovery could take years. In either scenario, the costs to the perpetrators are significantly lower than those associated with engaging in a traditional attack. Perhaps more importantly, estimates predicted that nineteen million individuals would know how to launch cyberattacks in 2002, making it likely that at the current time many more individuals will have acquired the knowledge and capability. It is now clear an elite hacker community exists and that the capabilities for IW are available to various individuals and nations, with the minimal entry requirement that the attacker have internet access. Attackers also gain an advantage when using IW because assaults can be routed through innocent intermediary telecommunications systems, making it extremely difficult to trace the effects back to the actual assailant. This potential anonymity may increase the attractiveness of IW to a group looking to attack asymmetrically.

Even when the resulting harm clearly qualifies as a serious attack and the attacker can be identified, separating cybercrime from IW actions can be difficult. Because a given IW attack can be ascribed to any of a large number of potential originators, victims will need to determine if an attack can be attributed

18 Schmitt, 37 Colum J Transnat L at 897 (cited in note 7).
19 Id.
20 Id at 898.
21 Id. See also Jennifer J. Rho, Comment, Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute, 7 Chi J Intl Law 695, 695 (2007) (noting that cybercriminals need only satellite phones, battery power, and computer access).
25 In order to provide the most efficient use of resources, servers will generally automatically route information through network channels to avoid overloading any given server. A casual internet user, then, may be in the US, requesting information from a server in France, having that information routed through any number of other servers en route. Because of this process, it can be difficult to trace a request all the way back to its source, particularly if the signal has been deliberately routed through a variety of servers around the world.
to the State that governs the origin point.\textsuperscript{26} Tied up in this inquiry are determinations of whether the attack would constitute an act of war between states or a criminal attack. Michael Schmitt, a prominent scholar on the subject, limits the definition of IW to actions taken during times of crisis against specific opponents,\textsuperscript{27} while reserving the concept of cybercrime for peacetime acts. However, with the prospect that a CNA could occur suddenly not as an isolated incident but as a precursor to a more serious attack,\textsuperscript{28} Professor Schmitt's distinction may not adequately serve our goal of distinguishing cybercrime and IW actions. Particularly in the long shadows of the 9/11 attacks and the ensuing (and continuing) "global war against terror," the distinction becomes less clear. The lack of such a distinction, however, might also be useful because it requires that all potential attacks and attackers be confronted as equal risks.

III. EXISTING INTERNATIONAL LAW AND ITS CHALLENGES IN THE CYBER WORLD

Current international laws, including the UN Charter, the protocols of the Geneva Convention, and existing multilateral treaties, attempt to govern the applications of IW and to limit its use. They do not, however, impose a ban on weapons designed to disrupt electronic communications.\textsuperscript{29} The lack of such a prohibition reflects an uncertainty in how to define international cybercrimes separately from IW, as well as an uncertainty about IW's potential value.

A. EXISTING INTERNATIONAL LAW

Existing international law in the area of cybercrime falls under three main umbrellas: the UN Charter, the Law of Armed Conflict ("LOAC"), and the Convention on Cybercrime. The UN Charter provides baseline law for interstate aggression, but is limited to considerations about force, which may not apply to cyberwarfare. LOAC conventions govern acts during wartime. The Convention on Cybercrime ("Convention") is a multilateral treaty that specifically addresses computer-related crime. However, the Convention gives states great flexibility in how they punish criminals.

\textsuperscript{26} Horace B. Robertson, Jr., Self-Defense against Computer Network Attack under International Law, 76 Intl L Stud 121, 122 (2002).
\textsuperscript{27} Schmitt, 37 Colum J Transnatl L at 891 (cited in note 7).
\textsuperscript{28} Robertson, 76 Intl L Stud at 141 (cited in note 26).
\textsuperscript{29} Roger D. Scott, Legal Aspects of Information Warfare: Military Disruption of Telecommunications, 45 Naval L Rev 57, 58 (1998).
1. The UN Charter

The UN Charter provides a baseline law for interstate aggression. Article 2(4) limits "the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent" with UN purposes, one of which is the maintenance of international peace and security. It is important to note, however, that although the UN has since clearly defined that aggression always constitutes a breach of the peace, it does not follow that a threat to the peace will always constitute aggression. In this context, peace is defined as the absence of the use of force; the lack of an inquiry into the legitimacy of other types of threats to peace highlights the weakness of such a limited definition.

The Charter’s Article 2(4) limitation does come with exceptions. Article 51 preserves "the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." This right of self-defense is restricted to responses to “armed attack”; permitted behavior under this restriction would be narrower than the “use of force” forbidden by Article 2(4). As such, a nation could suffer a use of force that does not qualify as “armed attack” and be forbidden the right of aggressive self-defense.

Acceptable self-defense under Article 51 usually takes two forms: reprisal and retorsion.

Acts of reprisal are actions that would, outside of a specific three-step process, be deemed illegal under the UN Charter. Justified state reprisals require (1) an assailant’s illegal act, followed by (2) the assailant refusing to satisfy (3) the victim state’s demand for redress. Retorsions generally consist of unfriendly but legal acts of retaliatory or coercive force. It is important to note that a
retorsion does not require an aggressive provocation.\textsuperscript{39} A retorsion in the IW context would be limited to responding against the system thought to be generating the attack. Power and telecommunications grids attached to the system would thus be off limits,\textsuperscript{40} and action targeting those systems is likely to fall more firmly under the zone of reprisal (assuming a demand for redress has been refused).

2. The Law of Armed Conflict

LOAC conventions\textsuperscript{41} govern the conduct of combatants during wartime, limiting acceptable attacks to military objectives.\textsuperscript{42} This LOAC restriction extends to the application of any offensive military capability and should extend as well to CNAs and other IW techniques.\textsuperscript{43} As might be expected in the CNA and IW context, however, some commentators argue that these weapons could legitimately target any militarily-related telecommunications because of the difficulty in separating military from nonmilitary uses of the technology.\textsuperscript{44}

LOAC also requires that combatants afford noncombatants special consideration. Protocol I of the Geneva Conventions ("Protocol I") requires that "the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."\textsuperscript{45} Protocol I also prohibits causing widespread, long-term damage to the environment, the starvation of civilians, and directing attacks against works and installations that "may cause the release of dangerous forces and consequent severe losses among the civilian population."\textsuperscript{46}

\textsuperscript{39} See id at 950 (noting the possibility of retorsion against parties without reasonable expectation to be punishing the actual perpetrators of the aggressive act).

\textsuperscript{40} Id at 951.

\textsuperscript{41} The LOAC conventions are a combination of treaties and customary international law, and they pull on scattered portions of the Geneva Conventions. For an example, see US Department of Defense, Directive 2311.01E (May 9, 2006), available online at <http://www.dtic.mil/whs/directives/corres/pdf/231101p.pdf> (visited Apr 5, 2008).

\textsuperscript{42} Scott, 45 Naval L Rev at 59 (cited in note 29).

\textsuperscript{43} Id.

\textsuperscript{44} See id.

\textsuperscript{45} Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art 48, 1125 UN Treaty Ser 3 (1979) ("Protocol I").

\textsuperscript{46} Id at arts 54–56.
3. The Convention on Cybercrime

The Council of Europe's Convention on Cybercrime ("Convention") represents the only legally binding multilateral instrument specifically addressing computer-related crime, advancing, "as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime." The Convention gives special attention to offenses including copyright infringement, computer-related fraud, child pornography, and offenses related to breaches of network security. The Convention, which has been signed by forty-three states and ratified by sixteen, also begins to shift the focus from punishing offenders to detecting and preventing computer crimes. For example, Chapter II, section 1's five substantive enumerated titles address protecting computer data and systems, computer-related fraud and forgery, content-related offenses, copyright infringement, and aiding and abetting.

In addition to establishing clear substantive offenses, the Convention employs flexible standards and relies on international cooperation to provide a starting point for addressing these offenses with criminal laws. The Convention achieves this step through its balance of mandatory and permissive language. Although the substantive provisions contain clear directives that parties to the agreement "shall adopt" laws to criminalize the behavior, the Convention provides for flexible interpretation of what the exact wording of those laws may be in two ways. First, it leaves to each party the determination of "legislative and other measures as may be necessary" to effect the necessary correct level of deterrence. Moreover, the exact requirements of the crimes are left to the

49 Romero, 14 Ind J L & Info Tech at 126 (cited in note 17).
50 Id.
51 Convention on Cybercrime, arts 2–6 (cited in note 48). Title 1 lists as violations the illegal accessing of computer systems (art 2), interception without right of nonpublic transmissions (art 3), data interference (art 4), the intentional hindering of a computer system's functionality (art 5), and creating or using devices which commit acts banned in Articles 2–5 (art 6).
52 Id, art 7–8. Title 2 addresses computer-related fraud (art 8) and the related offense of computer-related forgery (art 7).
53 Id, art 9. Title 3 addresses content-related offenses, specifically child pornography.
54 Id, art 10.
55 Id, art 11.
56 See, for example, id, arts 2–6.
57 Id, arts 2–13. Each substantive Article of the Convention begins with the phrase, "Each party shall adopt such legislative and other measures as may be necessary. . . ."
signatories as well; in the case of illegal interception, for example, each country “may require that the offence be committed with dishonest intent, or in relation to a computer system connected to another computer system.” The Convention also gives signatories incredible leeway in setting punishment, holding only that sanctions be “effective, proportionate and dissuasive,” without even requiring that the sanctions be criminal. The Convention also acknowledges “international co-operation” as its means of enforcing inter-territorial crimes. These flexible definitions allow the signatories to develop laws that reflect unique cultural preferences regarding criminality and punishment, while also establishing a baseline for the included offenses. Such an alignment provides a useful starting point for addressing these acts criminally (and expanding the scope of deterrence beyond the private civil suits allowed by Sosa v Alvarez-Machain), but at the same time it seems likely that these varying standards will not be enforced as readily as a new international law could.

B. CHALLENGES TO THE EXISTING LAW

The unique nature of IW raises special challenges to the existing law described above because of IW’s many forms and potential practitioners. Combined with the wide variety of beliefs that motivate the legislative bodies responsible for establishing a governing structure, IW’s natural variety has led to calls for a new normative framework. IW’s varied forms and outcomes pose particularly significant problems for attempts to expand the current law to include IW. These problems include questions about how the “use of force” provisions in the UN Charter apply to IW and how definitions of the physical world translate to acts committed in a world with its own unique constraints on action, as well as general uncertainty about what constitutes a legal military use of IW (an area in which extension by analogy has proven particularly fruitless).

1. On IW, the Use of Force, and the UN Charter

The first problem in applying existing law to IW arises because the baseline for determining the legality of aggressive action, the UN Charter and its use of force provisions, does not clearly address IW. The very nature of the attacks at issue, in fact, raises the question of whether certain types of IW will ever qualify

58 Id, art 3.
59 Id, art 13.
60 Id, art 23.
as "use of force" under a conventional understanding of the term.\textsuperscript{63} The language of Article 2(4) aggravates the confusion by prohibiting only "armed force." Other portions of the Charter refer without qualification to "force" and have been construed to allow certain types of pressure to be exerted without violating the armed force prohibition clause.\textsuperscript{64} While economic and political coercion might constitute threats to international stability without amounting to a use of force, such a distinction does not provide any guidance in determining the legality of an act of IW that has no physical effects. This ambiguity is problematic because the use-of-force standard's "armed force" measurement has traditionally separated lesser threats to international stability from redressable acts,\textsuperscript{65} and IW without physical effects would thus seem hard to identify on the traditional measurement. Some commentators have argued, however, that IW can in certain circumstances present the type of threat typically associated with an act of armed force (despite only interfering with communications) by amounting to a type of coercion specifically sanctioned by Article 41 of the UN Charter.\textsuperscript{66}

In addition to failing to provide a clear test to measure the legality of IW, the multiple forms and potential assailants who could engage in IW make measuring the threshold criteria more difficult. An attack that is rapidly and remotely initiated by one individual, or a small group of individuals scattered throughout the world, may not clearly qualify as a use of force under the Charter.\textsuperscript{67} Assailants' ability to initiate attacks with an initial degree of anonymity adds to the problem that they may be both remotely located and dispersed in multiple locales. Even if the attack created results that clearly violated the armed force prohibitions of the UN Charter, a victim would be hard pressed to use justified self-defense under Article 51 because of an inability to identify the assailants. This challenge has led some commentators to argue for a looser reading of Article 51 that allows for anticipatory self-defense against IW.\textsuperscript{68} This

\textsuperscript{63} Id at 904.
\textsuperscript{64} For a general discussion, see id at 906.
\textsuperscript{65} Id at 904.
\textsuperscript{66} Robertson, 76 Intl L Stud at 137–38 (cited in note 26) (arguing that Article 41 is not fully preclusive of categorizing CNA as armed force, but in doing so relies on the assertion that "the 'complete or partial interruption' of [computer networks controlling vital societal functions or critical national-security functions] would have a much more drastic effect than anything that could have been envisaged by the framers of the Charter in 1945").
\textsuperscript{67} Id at 122.
\textsuperscript{68} For a general discussion, see id; see also Walter Gary Sharp, Sr., CyberSpace and the Use of Force 130 (Aegis Research 1999) for a discussion of the inquiry into the necessary hostile intent to justify retaliatory action. Such actions, however, could include shutting down servers suspected of hosting the attack.
debate clarifies the problems IW poses to the existing law contained in the UN Charter: the uncertainty of how to classify IW in regard to the conventional framework makes attempts to apply the laws of that framework an almost Sisyphean task.

2. Military Application and Uncertainty

One result of any eventual IW law will be to provide military officers with a clear understanding of when the use of IW is legally acceptable and how those attacks should be conducted and targeted to avoid violating LOAC principles. Unfortunately, existing law does not provide such certainty. IW provides a finely discriminating tool to combatants that may aid in protecting innocent lives and minimizing the collateral damage of military operations.\(^6\) This capability argues against an outright ban on IW and weighs against other rules that run the risk of being overbroad.

With the process of distinguishing between legitimate and illegitimate weapons growing more difficult,\(^7\) muddled rules could lead to military decisions underutilizing IW, increasing the social costs of the altercation. The difficulty in establishing the difference between a combatant and a noncombatant also increases, as any individual with computer access could suddenly become a potential combatant. IW reprisals over electronic networks could inadvertently target innocent noncombatants, and fear of reprisal for illegal action could incentivize commanders to replace IW methods with costlier conventional techniques. Rather than failing to discriminate between combatants and noncombatants, militaries could expend increased resources in tracking and neutralizing enemy combatants via conventional means.

3. Natural Properties of Cyberspace and Existing Law’s Failure to Provide for Them

The challenges highlighted in applying UN Charter law to IW hint at a broader problem, namely that information technology operates according to a separate set of constraints than the ones governing traditional kinetic action. Existing law assumes that actions will be bound by the physical constraints of time and space, and perhaps more importantly assumes that the consequences of any action will manifest themselves via a physical effect on other objects within

\(^6\) For example, temporarily disabling a power grid via CNA will lower reconstruction costs in comparison to the destruction of the grid or power plant via traditional weapons. See Shulman, 37 Colum Transnatl L at 942–43 (cited in note 10).

\(^7\) Id at 940.
these assumed boundaries.\textsuperscript{71} IW, however, presents an area in which these assumptions, while not assuredly false, do not remain perpetually true.

The move to cyberspace creates a new balance of power. Conventional symbols of strength, whether economic, military, or diplomatic, do not operate as readily when physical power is effectively useless. In many instances, the sheer force of numbers is equally irrelevant to deciding which of two combatants has the upper hand in a cyberspace conflict. An organization with no hope of effecting a change in the traditional, physical world can create an entirely level playing field in this new terrain. Perhaps more importantly, constantly improving technology may make it possible for an individual to establish parity with a traditional superpower.\textsuperscript{72} Existing law struggles to take into account this vision of power because to do so would require affording to every individual a level of deference traditionally reserved for the state, without any recourse to visible boundaries or characteristics. Rather than transacting with one or several states or the inhabitants of a physical region, cyberspace allows groups to form based on ideology, interest, or to not form at all, leaving an individual to act self-interestedly but with the potential power traditionally reserved for a state.

This shift is important because it draws out the problems of governing behavior that has been traditionally restricted to one set of actors (states) in limited circumstances (war), but which is now almost fully accessible to anyone. Conventional war involves conflict between states acting on behalf of the interests of geographically identifiable groups. Furthermore, during war, states and their agents are authorized to engage in behavior that would be prohibited under other circumstances. In the process of translating acceptable behavior to the altered power dynamic of the cybersphere, however, this understanding would require affording the privileges of states at war to any actor involved in the conflict. This extension would be done without a clear understanding of which acts would be legal, however, because certain acts may not carry results which would trigger the justification of conventional laws.

The disconnect between the traditional worldview and the potential translations to the cybersphere highlights the weakness of the Convention on Cybercrime. The need for some level of standardized international law governing these crimes has been established, but the problem remains of

\textsuperscript{71} Rho, 7 Chi J Intl L at 706 (cited in note 21).

\textsuperscript{72} While it is unlikely that a lone individual would take on the US, the fact remains that individuals creating viruses have caused immense damage without assistance, and could, at least formally, create such a scenario. Moreover, because the individual could be anywhere in the world, traditional remedies may be unavailable to the US or another victim state. See note 73 for such an example.
drawing the line between individuals operating as criminals and individuals operating as combatants.

The “I Love You” virus highlights the potential problems the Convention fails to address. Unleashed by hackers in the Philippines, the “I Love You” virus caused infected computers to send e-mails to all the contacts in the computer’s hard drive. The virus then repeated the process when recipients opened the file. The aggregate economic damage from the virus was estimated at between ten and eleven billion dollars. Analyzing the situation that surrounded the “I Love You” virus under three alternative situations provides a firmer idea of how the Convention struggles in application to deter illegal IW.

Assume all of the following three scenarios take place in a fully compliant signatory of the Convention. In the first situation, the virus is created and disseminated by an individual. In the second, the perpetrators are a group composed entirely of citizens acting entirely within the territory of one state. In the third, the group is made up of citizens of multiple nationalities, and only the creator, and not the individuals who actually unleashed the virus, resides in or is present in the state. In this situation, it may be that the rest of the group is spread throughout a variety of both signatory and nonsignatory states, making chances slim that the remainder of the group can be identified and tracked down even within the signatory states.

While the Convention clearly covers the first two scenarios and provides a criminal remedy against the individuals, there remains the chance for complications. Separate nations may disagree on the appropriate nature of punishment or what constitutes the “dishonest intent” required by the Convention. In such an eventuality, while a form of justice may be reached, there is no guarantee that the outcome will provide any greater satisfaction than what happened with the “I Love You” virus. The third example raises a host of complications, and the Convention falls back on “international cooperation” as...
the proffered solution to all of them.\textsuperscript{76} The outcome will require that the victim nation is satisfied with the sanctions legislated by each member country\textsuperscript{77} and that appropriate agreements can be worked out with any nonsignatory state to ensure punishment for members of the group identified and located within its borders. With such a wide possible range of standards, however, the potential for the same uncertainty which poses problems for the LOAC analysis re-emerges. This uncertainty may be more important to resolve than questions of distinguishing legal acts of war from illegal criminal acts when they are committed by nonstate actors. While the Convention thus works well in certain limited situations, its ability to effectively govern IW is decidedly unclear, in both its current form and, to some extent, in a variety of potential permutations.

The US decision to join the Convention on Cybercrime's signatories in 2006,\textsuperscript{78} despite some assertions that US law may already be comprehensive,\textsuperscript{79} highlights the unbounded nature of cybercrime and information attacks when viewed with an eye towards traditional restrictions, particularly geographical and physical constraints.\textsuperscript{80} If existing US law could independently address these issues, the move to join the Convention would be unlikely. Signing may then indicate that even a comprehensive law may not succeed if it only works domestically, and the decision to sign may be read as an acknowledgement of the need for international standards. The move may also push towards establishing the Convention as a customary international norm. Gaining an increased number of signatories would assist in establishing the Convention as state practice and would lead towards the conclusion that a legal obligation exists, satisfying the \textit{opinio juris} requirement. Looking forward, establishing such a customary international norm would allow for jurisdiction in US federal courts and assist in allowing civil actions to be brought against perpetrators.\textsuperscript{81}

\textsuperscript{76} Convention on Cybercrime, Preamble ¶ 4 (cited in note 48).
\textsuperscript{77} See id, art 13.
\textsuperscript{79} See Shulman, 37 Colum Transnat L at 952 (cited in note 10).
\textsuperscript{80} Rho, 7 Chi J Intl L at 695 (cited in note 21).
\textsuperscript{81} See id at 696 for a discussion of \textit{Sosa} (establishing federal jurisdiction over private suits regardless of plaintiff and defendant nationality where the violation of customary international norms is incorporated into federal law by the Alien Tort Statute).
The various frameworks offered for a governing law of IO share the common feature of relying on a state-based international structure. Proponents of frameworks based on both international treaties and customary international law have relied on structures characterized by the exclusive participation of states in developing law. Christiana Ochoa attributes this tendency to the traditional narrative of international law, in which "states are sovereign, enjoy a monopoly on legal personality under international law, and make international law." This traditional approach assigns the means of establishing any form of law exclusively to nations and leaves it to them to determine whether to achieve this end via international treaties (such as the Convention on Cybercrime) or more informally. The informal approach of allowing norms to develop, however, has also typically relied on a state-based approach, incorporating both the subjective and objective components of state practice and opinio juris into its formation.

Recent commentary on customary international law formation, however, has suggested that a realist perspective on this subject requires an analysis of the role of nonstate actors in the formation process. The underlying principle of this perspective rests on the idea that those bound by international law ought to have a voice in its formation. How completely to democratize the process has been debated, with some arguing for an inclusion of states, intergovernmental organizations, and nongovernmental organizations ("NGOs"). Others have
approached NGOs with skepticism, with concerns that NGOs may be overly politicized.\textsuperscript{87} NGOs may not, therefore, be the best proxies for civil society in the nonstate-based, participatory process of law formation.\textsuperscript{88}

The realist perspective is supported by current practices that reinforce, at least, its assertion that the process of forming a new governing law for IW by custom should look beyond state actors. Individuals may now enforce laws protecting human rights at the national and international level.\textsuperscript{89} The recent passage of the Declaration on the Rights of Indigenous Peoples, a document designed to help shape the formation of custom and international law by establishing an international precedent, allows for indigenous groups to self-identify and to assert their rights.\textsuperscript{90} This document also reflects the work of states and NGOs, evidencing the possibility of law created outside of an exclusively state-based framework.\textsuperscript{91} While allowing an NGO to participate may not appear novel at first, it runs counter to an asserted trend in the traditional customary international law literature. The traditional approach would stop short of recognizing nonstate actors' role in law formation and restrict participation exclusively to states.\textsuperscript{92}

The components of customary international law, moreover—state practice and \textit{opinio juris}—do not pose an insurmountable challenge to the idea that individuals should participate in its formation. By looking at the larger purpose of the two components, the inclusion of both objective and subjective elements in this type of law, it becomes clear that individuals can and most likely do participate in the creation of similar components in the already established law.\textsuperscript{93}

\textsuperscript{87} See id at 179.
\textsuperscript{88} Id at 147–48.
\textsuperscript{89} Id at 155.
\textsuperscript{92} Ochoa, 48 Va J Intl L at 138 (cited in note 5).
\textsuperscript{93} For example, courts already look to public opinion to interpret text reasonably and avoid absurd results, even though public opinion is not a "state-based" creation, but rather an amalgamation of views of individuals. See id at 175. See also Hari M. Osofsky and Janet Koven Levit, \textit{The Scale of Networks?: Local Climate Change Coalitions}, 8 Chi J Intl L 409, 428–31 (2008) for a discussion of bottom-up lawmaking in the context of climate change.
B. THE "NEW" CUSTOMARY INTERNATIONAL LAW AND IO

With other areas of law employing versions of the realist perspective on customary international law formation, the potential of this perspective to assist in developing a governing law for IO merits evaluation. This analysis will be limited to the potential for a nonstate-based method of formation to serve as a structural guide and will not venture into the substance of such a potential law. The possibility of allowing a broader range of voices into the process does present some potentially significant advantages, including navigating the more troublesome aspects of the "use of force," developing a law that recognizes the altered power structures in a networked world, and improving understanding between developed and emerging nations. Using a nonstate-based process for customary international law formation could allow the development of norms that address IO and CNA apart from the use of force implications that struggle to constrain it at present. The inclusion of nonstate voices in the process allows for the potential of a bottom-up lawmaking process that may identify and negotiate around factors that private actors value and that nation-states who may prioritize continuity with UN Charter provisions have ignored. Such a process may also allow for important influences on the technology to be heard: the UN Working Group on Internet Governance has noted that the multiplicity of stakeholders in IO often leads to solutions based on a limited selection of the important interests, but without the input of all stakeholders. In addition, bottom-up lawmaking would also react to the growing recognition of the need to include all stakeholders.

A particularly large benefit of such a process is the way in which a nonstate-based formation process could account for the power-shifting problems that plague ideas about internet governance as discussed above. By

94 See, for example, id at 157 (discussing the participation of individuals, separate from NGOs, in the creation of the United Nations' Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights).
95 A further analysis of the policy implications of such a structure deserves a fuller treatment and may highlight benefits and disadvantages from such a process that will not be addressed here.
96 See Section III.B.1.
97 Schmitt, 37 Colum J Transnat L at 922 (cited in note 7).
98 Ochoa, 48 Va J Intl L at 148 (cited in note 5) (noting studies in trade-finance communities in which private actors and public actors in the trade finance sector have set rules that have congealed into hard law with legal consequences).
100 Willy Jensen, Internet Governance: Striking the Appropriate Balance between All Stakeholders, in Drake, ed, Reforming Internet Governance 35, 35 (cited in note 99).
allowing nonstate actors to participate in the formation of the law, the process may recognize the balance of power that exists in the governed territory. Allowing parties to self-identify on grounds beyond nationality addresses two concerns. First, it recognizes the growing tendency towards cross-border group formation.\textsuperscript{101} Second, it creates a mechanism for such groups, which might remain anonymous in a state of the world in which they are disenfranchised, to identify themselves to other parties. The result of this identification can be both to increase communication between all interested groups (which could lead to better adapted and more enforceable laws) and to reduce the costs of identifying participants in the event of a breach of those norms. Allowing nonstate actors to participate in the process may also enhance the acceptance of any formed law in the long-term by incorporating the socio-economic interests of small nonstate groups or individuals. These interests may also provide closer analogs to the interests of developing countries and emerging economies than established states and superpowers are currently able to achieve because established states represent a different interest set that may not account for the needs of countries that have not yet become major users of the internet.\textsuperscript{102} Such results will not necessarily be reciprocal, however, indicating that continued reliance on a state-based approach—even one that involves developing countries—may not bring forward the concerns of nonstate groups.

Economic reasoning may also offer increased incentives to engage in this revised understanding of customary international law formation. Forcing states to interact with emerging nations, international groups, and individuals can generate an increase in role reversibility.\textsuperscript{103} By allowing the concerns of smaller parties from a range of backgrounds, it becomes more likely that parties will be forced to account for the needs and desires of all because, in a nice symmetry with the matter discussed, these smaller groups will have equal power to speak and to improve the understanding larger groups have of their respective situations. In the case of the internet, such an exchange could lead to governance that more closely aligns to the possibilities of the technology in areas including use, capability, and identification. Nation-states may similarly benefit by gaining the ability to bring information on new technologies into the discussion, allowing for the law to address technological advances proactively by providing incentives to innovators to collaborate and to share information. The interaction is also likely to force participants to articulate concerns, which should generate clearer norms by forcing increased discussion and reaction to these apprehensions.

\textsuperscript{101} Ochoa, 48 Va J Intl L at 167–68 (cited in note 5).

\textsuperscript{102} Jensen, \textit{Internet Governance} at 37 (cited in note 100).

There are immediate concerns about the efficacy of such a system, however. Traditionally, customary international law has evolved over long periods of time, which has led to some dismissal of its viability as a means for developing law in this area.\textsuperscript{104} There are also challenges to its ability to adapt to the changing technology. Determining which individuals could participate in developing a governing law may also encounter resistance as a matter of policy.\textsuperscript{105} The highly accessible nature of the internet could lead to an overly democratic process, with different parties attempting to assert themselves in the process. Such an issue raises questions of the establishment of a qualifying body to determine who may receive a seat at the table. This weeding out process could be controversial and runs the risk of prematurely stunting the process. Moreover, there remains the question of whether such a process can fully address the limitations embodied by existing law, or if such a process, even if theoretically viable, will be functionally useful.\textsuperscript{106}

Some of these concerns may be overstated. While customary international law has generally developed over longer periods of time, recent agreements on such a law to govern outer space have been quickly agreed on and implemented.\textsuperscript{107} Although the low-entry costs to IW will necessitate a greater number of participants in developing the law, there seems little reason to believe that once an agreement is reached, practice and custom could not be more readily viewed as having coalesced into legally enforceable customary norms. In fact, the opposite seems more likely. By allowing a greater amount of participation by affected organizations and individuals, a stronger argument can be made that any agreement reflects an agreed upon behavioral norm for IW. As such, it can be viewed as creating a legal obligation for participants, which

\textsuperscript{104} See Schmitt, 37 Colum J Transnatl L at 921 (cited in note 7).
\textsuperscript{105} Politicians may be reluctant to be viewed as allowing a voice to any individual or group based on destructive capabilities; a simple example would be the policy of refusing to negotiate with terrorists. This reluctance, however, reflects the need for a paradigm shift away from the state-based conception of international law; politicians must recognize that a shift away from state-based law will involve affording privileges to groups that previously would not have received them.
\textsuperscript{106} Such a process will require high levels of cooperation and interaction on an international level; it is unclear whether these levels can be achieved and maintained.
should lead to a more rapid acknowledgement of its role as customary international law.

Concerns regarding the potentially large number of participants should also not be deemed prohibitive without further analysis of whether a more inclusive process will really attract too many participants or if the nature of the concerns will serve as an effective filter that leads to only greatly affected organizations participating. These concerns are largely based on ideas of transaction costs, which increase with the number of participants. At the same time, however, the increase seems likely to force groups and individuals with only limited interest in the outcomes of the discussions to entrust them to stakeholders with higher levels of concern. As such, the fear that such a method will lead to an unmanageably large number of participants with completely prohibitive costs will potentially be self-addressing, leading to a discussion group with concrete stakes in the outcome.

V. CONCLUSION

The reality of IO accessibility, and the variety of IW capabilities, makes a governing law for IO a necessity. This Development stops short of suggesting the goals or substance of such a law, but recognizes that whatever those goals may be, existing law seems unable to cope with the potential harms presented by IO. Existing law also seems resistant to ready adoption and application in the sphere of IO, and a thorough re-evaluative process is required in determining new law. The nature of cyberspace itself further complicates the process by offering a realm that challenges traditional notions of power and requires an acceptance of previously undreamt global equality. At the same time, the emergence of a realist view of customary international law formation that advocates the role of individuals in developing laws presents a possible method which has distinct benefits and restrictions. This view merits further study to determine whether or not a policy recommendation can be made regarding its viability as a tool for developing the substance of a new law.