WHY STATES NEED AN INTERNATIONAL LAW FOR INFORMATION OPERATIONS

by
Duncan B. Hollis[*]

Just as states have spent the last several years wrestling with the appropriate legal response to terror, they must now undertake a similar effort to deal with the burgeoning use of "information operations" (IO). IO involves the use of information technology, such as computer network attacks or psychological operations, to influence, disrupt, corrupt, usurp, or defend information systems and the infrastructure they support. More than thirty states have developed IO capacities. But IO is also undoubtedly attractive to non-state actors like al-Qaeda, since the technology is mostly inexpensive, easy-to-use, and capable of deployment from virtually anywhere.

This Article assesses the ways in which international law—specifically the rules regulating the use of force and the law of war—currently applies to IO. Conventional wisdom suggests existing rules can cover IO by analogy. The conventional wisdom is only half-right. This Article explains why the existing rules govern IO, but challenges the unstated assumption that they do so appropriately. Translating existing rules into the IO context produces extensive uncertainty, risking unintentional escalations of conflict where forces have differing interpretations of what is permissible. Alternatively, such uncertainty may discourage the use of IO even if it might produce less harm than traditional means of warfare. Beyond uncertainty, the existing legal framework is insufficient and overly complex. Existing rules have little to say about the non-state actors that will be at the center of future conflicts. And where the laws of war do not apply—even by analogy—an overwhelmingly complex set of other international and foreign laws purport to govern IO.

To remedy such deficiencies, this Article proposes a new legal framework—an international law for information operations (ILIO). By adopting an ILIO, states could alleviate the uncertainty and complexity of the status quo,

[*] Associate Professor of Law, Temple University Beasley School of Law, and, from 1998–2004, Attorney Adviser, Office of the Legal Adviser, U.S. Department of State. I want to thank Jeffrey Dunoff, Craig Green, David Hoffman, David Kaye, Jaya Ramji-Nogales, and Peter Spiro for valuable comments on earlier drafts, as well as the organizers of the April 2007 Symposium on War, War Crimes, and the War on Terrorism at Lewis & Clark Law School, for which I originally prepared this Article. Since then, I have revised the Article to reflect recent events in Estonia. The Article also incorporates my work for a military audience on information operations, which will appear in the Marine Corps Foundation-sponsored book, *The War for the Message* (forthcoming 2008). Finally, I extend my heartfelt appreciation to George Deeney, Joshua Newcomer, and Maria Murphy for their research assistance with this project.

reduce transaction costs for states fighting global terror, and lessen the collateral costs of armed conflict itself. This Article concludes with a review of some of the regulatory design questions facing an ILIO, but does not offer any specific rules. Rather, its ultimate aim is to convince states and scholars about the need for an ILIO in the first place.

I. INTRODUCTION

For three weeks in 2007, Estonia claimed to be under attack. No bombs, missiles, or conventional forces threatened the small Baltic nation. Rather, the assault came over the Internet. It began on April 27, the day Estonia relocated a Soviet-era war memorial from the center of its capital, Tallinn; a move vociferously opposed by the Russian government and Estonia's ethnic Russian population.[1] In apparent retaliation, data requests from thousands of computers flooded and overwhelmed Estonian websites, making them inaccessible for various periods of time.[2]

[1] Steven Lee Myers, '*E-stonia' Accuses Russia of Computer Attacks,* N.Y. TIMES, May 18, 2007, http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?h. Russians view the relocated bronze statue as a memorial to Soviet soldiers who died fighting Nazi Germany, while many Estonians view it as a reminder of foreign occupation. Russia termed the relocation "blasphemy" and called for the Estonian government's resignation. It reduced freight train service and suspended passenger service for purported track repairs. Ethnic Russians rioted in Estonia, leading to hundreds of arrests and one death. In Moscow, protestors rushed Estonia's ambassador at a news conference, prompting the use of pepper spray by the ambassador's security detail. Protestors also blockaded Estonia's embassy, until a German-brokered "holiday" for Estonia's ambassador brought the stand-off to an end. *See id.*; Alex Rodriguez, *Attacks on Estonia Move to New Front,* CHI. TRIB., May 29, 2007; *Estonia and Russia: A Cyber-Riot*, ECONOMIST, May 12, 2007.

[2] Known in technical circles as a "distributed denial-of-service attack," this method clogs not only a state's servers, but its routers and switches as well—"the specialized devices that direct traffic on the network." Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1.

The queries came in coordinated and increasingly larger waves, knocking out Estonian government websites first, including the Prime Minister's and President's offices as well as the Justice and Foreign Ministries. Members of Estonia's Parliament went four days without e-mail.[3] By the May 8–9 celebrations of Nazi Germany's defeat, the targets had broadened to include daily newspapers, television stations, Internet service providers, universities, hospitals, and banks.[4] Estonian telephone exchanges received data "bombs," disabling emergency phone numbers for paramedic and fire services for over an hour.[5] Ultimately, more than a million computers were employed against Estonia through the use of "botnets"—ordinary computers hijacked by viruses to perform such attacks without their owner's knowledge.[6] Estonia's largest bank had to suspend online services for ninety minutes, and eventually barred all foreign access to its servers. Other sites did the same, with obvious economic and political consequences.[7]

Senior Estonian officials quickly implicated the Russian government in these acts, noting that the attacks prevented Estonia from countering Russian propaganda and making its case to the world.[8] At least one Internet address involved in the initial wave belonged to an official in Russian President Putin's administration.[9] The Kremlin denied any involvement, however, invoking the ability of hackers to manipulate computers remotely.[10] Whether or not the Russian government had any role, networks of ethnic Russian "hactivists"—technical experts unconnected to a government—played a significant role in encouraging and participating in the digital disruption.[11]

Estonia's experience marked the first time a nation-state has faced such an overt, coordinated, and extensive assault on its information networks.[12] Estonian officials claimed that they were the victim of a new

---

[3] *Id.*

[4] *Id.*; Myers, *supra* note 1; Peter Finn, *Cyber Attacks Stalk Estonia*, WASH. POST, May 19, 2007.

[5] *Newly Nasty*, ECONOMIST, May 24, 2007, *available at* http://www.economist.com/world/international/displaystory.cfm?story_id=9228757.

[6] *Estonia and Russia*, *supra* note 1; Myers, *supra* note 1.

[7] Myers, *supra* note 1.

[8] *Newly Nasty, supra* note 5; Robert Anderson et al., *US Warns Cyber-attacks Will Increase*, FIN. TIMES, May 18, 2007, at 12.

[9] Landler & Markoff, *supra* note 2.

[10] *Id.*; *Estonian Links Moscow to Internet Attack*, N.Y. TIMES, May 18, 2007, at A12; Finn, *supra* note 4.

[11] *See* John Schwartz, *When Computers Attack,* N.Y. TIMES, June 24, 2007, at 1.

[12] *Newly Nasty, supra* note 5. Prior instances of digital attacks against states had primarily involved probing a state's Internet defenses for entry points, rather than blocking access to them. *Id.*; Bradley Graham, *Hackers Attack Via Chinese Web Sites*, WASH. POST, Aug. 25, 2005, at A1 (describing websites in China being used to try to breach U.S. federal government unclassified computer networks). Most discussions of conflicts in cyberspace to date have focused on hypotheticals or individual cases where unidentified hackers have accessed or attacked government computer

form of combat—cyberwarfare.[13] Estonia's Defense Minister Jaak Aviksoo insisted that such sabotage "cannot be treated as hooliganism, but has to be treated as an attack against the state."[14] As Estonia's Defense Ministry Spokesperson explained, "If you have a missile attack against, let's say, an airport, it is an act of war. . . . If the same result is caused by computers, then how else do you describe that kind of attack?"[15] Other observers, however, denied that Estonia's experience qualified as warfare, suggesting the attacks' hactivist sources were no different from similar data deluges perpetrated against private corporations and information networks over the last several years.[16] Although disruptive, the attacks on Estonia had caused neither terror nor destruction.[17] In this sense, the attacks could be deemed merely criminal. And Estonia apparently agreed with that characterization, treating the acts as not only war-like, but also launching a criminal investigation to locate and prosecute those responsible.[18] In the incident's latest chapter, Estonia and Russia have sparred over questions of Russia's duty to deny a safe haven to the attackers and its obligation to assist Estonia in locating those responsible under a bilateral mutual legal assistance treaty.[19]

The question of whether the Estonia attacks qualify as crimes, acts of war, or both, mirrors the dilemma faced in trying to decide how best to respond to transnational terror. In the terrorism context, four approaches have emerged. The first approach treats terrorism as a crime,

networks. *See, e.g.*, Sean M. Condron, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 404–05 (2007) (describing hacker attacks apparently from China against Taiwan and U.S. federal government computer systems); Jennifer J. Rho, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute,* 7 CHI. J. INT'L L. 695 (2007) (describing U.S. military field exercise involving an information attack on military and civilian infrastructures); Jason Barkham, *Information Warfare and International Law on the Use of Force,* 34 N.Y.U. J. INT'L L. & POL. 57, 68 (2001) (describing "Solar Sunrise" operation in which "two U.S. teenagers, aided by an Israeli, penetrated hundreds of U.S. Air Force computer systems" in February 1998).

[13] Myers, *supra* note 1; Landler & Markoff, *supra* note 2.

[14] Anderson et al., *supra* note 8.

[15] Myers, *supra* note 1 (quoting Madis Mikko). Estonian officials also compared the effects of these computer attacks to those from the closure of its ports to the sea. *See* Landler & Markoff, *supra* note 2.

[16] *See* Schwartz, *supra* note 11; *see also* Barkham, *supra* note 12, at 63 (describing a February 2000 denial of service attack that disabled some of the most popular sites on the Internet, including eBay, Yahoo!, and Amazon.com).

[17] *Federal Information Technology Security: Hearing Before the H. Comm. of Oversight and Government Reform* (2007), *available at* 2007 WLNR 10706849 (testimony of James A. Lewis, Senior Fellow and Director, Center for Strategic and International Studies).

[18] *Russia, Estonia Disagree over Cyber Attacks Investigation*, WORLD NEWS CONNECTIONS, July 13, 2007, *available at* Westlaw, 7/13/07 WRLDNWSC 21:01:03.

[19] *Id.* (Estonia claims that Russia withheld legal assistance to track down those responsible for the cyberattacks; Russia says that Estonia's request did not conform to their bilateral legal assistance treaty, and asked that Estonia format its request properly to encompass procedural, rather than investigative, assistance); *see also* Rodriguez, *supra* note 1; Finn, *supra* note 4.

susceptible to the tools (and restraints) of the criminal justice system.[20] A second approach characterizes the fight against global terrorism as war, with any legal restraints on the conflict provided by the existing law of war.[21] A third approach takes a middle path, suggesting that the war and crime paradigms are not mutually exclusive and favoring the employment of both in responding to the terror threat.[22] A fourth approach argues that terrorism qualifies neither as an act of war nor a crime, but as something new, which requires a new legal framework to combat it effectively.[23] Elements of the first three approaches are already

[20] *See, e.g.*, Leila Nadya Sadat, *Terrorism and the Rule of Law*, 3 WASH. U. GLOBAL STUD. L. REV. 135, 140 (2004) (arguing that transnational terrorists are not engaged in "armed conflict" under the law of war, but in organized crime); David Cole, *The New McCarthyism: Repeating History in the War on Terrorism*, 38 HARV. C.R.-C.L. L. REV. 1, 30 (2003) (suggesting that the safeguards of the criminal process should be treated as a necessary part of the "war on terrorism"); Jordan J. Paust, *War and Enemy Status After 9/11: Attacks on the Laws of War*, 28 YALE J. INT'L L. 325, 326–28 (2003) (rejecting claims of a U.S. "war" with al-Qaeda or terrorism, and suggesting that such a label has dangerous implications for acts that otherwise should be criminal).

[21] *See, e.g.,* President George W. Bush, Address Before a Joint Session of the Congress on the State of the Union, 40 WEEKLY COMP. PRES. DOC. 94, 96 (Jan. 20, 2004) ("[S]ome people question if America is really in a war at all. They view terrorism more as a crime, a problem to be solved mainly with law enforcement and indictments. . . . After the chaos and carnage of September the 11th, it is not enough to serve our enemies with legal papers. The terrorists and their supporters declared war on the United States, and war is what they got."). *See also* John Yoo, *Courts at War*, 91 CORNELL L. REV. 573, 578–79, 601 (2006) (arguing conflict with al-Qaeda truly is war); Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 HARV. L. REV. 2047, 2070–71 (2005) (rejecting U.S. courts' ability to question conflict against terrorism as "war" when political branches regard it as such); John C. Yoo & James C. Ho, *The Status of Terrorists*, 44 VA. J. INT'L L. 207, 213 (2003) (denying conflict with al-Qaeda is a "massive crime, rather than an act of war"); Ronald J. Sievert, *War on Terrorism or Global Law Enforcement Operation?,* 78 NOTRE DAME L. REV. 307, 351–52 (2003) (arguing for a predominantly military approach to anti-terrorism).

[22] *See, e.g.*, Mark A. Drumbl, *"Lesser Evils" in the War on Terrorism*, 36 CASE W. RES. J. INT'L L. 335, 335–36 (2004) (endorsing use of criminal law and military means to combat terrorism); Noah Feldman, *Choices of Law, Choices of War*, 25 HARV. J.L. & PUB. POL'Y 457, 457–58, 484–85 (2002) (finding that terrorism qualifies as both crime and war, undermining "the binary character of the war/crime" dichotomy and suggesting that neither should serve as the exclusive responsive framework); Sean D. Murphy, *Terrorism and the Concept of "Armed Attack" in Article 51 of the U.N. Charter*, 43 HARV. INT'L L.J. 41, 49 (2002) [hereinafter *Armed Attack*] (characterizing September 11, 2001 attacks "as *both* a criminal act and an armed attack").

[23] *See, e.g.*, Kenneth Anderson, *U.S. Counterterrorism Policy and Superpower Compliance with International Human Rights Norms*, 30 FORDHAM INT'L L.J. 455, 476–77 (2007) (advocating for new domestic—as opposed to international—legal regimes to combat terrorism); Bruce Ackerman, *This Is Not a War*, 113 YALE L.J. 1871, 1873 (2004) (seeking a third framework in lieu of the war/crime dichotomy); Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 761 (2004) (suggesting that we lack an adequate international legal paradigm for redressing the rise of global terrorism, and proposing a reconsideration of the law of armed conflict in concert with international human rights law).

evident in the cyberspace context. But on closer examination, the fourth approach—devising a new legal framework—may offer the most effective response to the challenges of regulating cyberspace conflicts.

To date, much as it did in the terrorism context before September 11, 2001, an approach based on criminal law has prevailed in responding to computer attacks.[24] As technology proliferated, nation-states adapted their domestic laws to criminalize various forms of "cybercrime" and to regulate how their law enforcement could employ new technologies.[25] In international law, states took the same approach. In 2001, the Council of Europe concluded the Convention on Cybercrime, in which the parties agreed to criminalize under their domestic laws certain attacks on computers and to improve methods of cooperation in investigating cybercrime.[26]

Estonia, however, broke away from a solely criminal law approach, by characterizing the attacks as an "act of war." As a member of the North Atlantic Treaty Organization (NATO), it called on that organization for assistance.[27] Although NATO states did not regard the episode as triggering the Treaty's collective defense obligations, the organization sent an expert to Estonia to observe the incident, and NATO ministers have agreed to study the issue further.[28] Thus, if the Estonia incident is any predictor for the future, cyberspace will become an arena for the use of military force and the law of war, whether in conjunction with, or in lieu of, existing criminal law frameworks.

Over the last decade, military thinkers have devised and developed a term—information operations (IO)—anticipating this "new category of warfare" that grows from the Internet's interconnectivity and other new

[24] Condron, *supra* note 12, at 407 ("Despite the magnitude of [the] threat, the United States currently operates under the presumption that a cyber attack constitutes a criminal activity, not a threat to national security.").

[25] *See, e.g.*, 18 U.S.C. § 1030 (2000) (U.S. federal law criminalizing fraud and related activity in connection with computers); 18 U.S.C. §§ 2510–2511 (2000) (U.S. federal laws regulating wire and electronic communication interceptions and interceptions of oral communications); *see generally* Richard W. Downing, *Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime*, 43 COLUM. J. TRANSNAT'L L. 705 (2005).

[26] Council of Europe, Convention on Cybercrime, C.E.T.S. No. 185 (Nov. 23, 2001), *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [hereinafter Cybercrime Convention].

[27] North Atlantic Treaty, art. 5, Apr. 4, 1949, 63 Stat. 2241, 2244 ("The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all; and consequently they agree that, if such an armed attack occurs, each of them . . . will assist the Party or Parties so attacked . . . .").

[28] Jim Michaels, *NATO to Study Defense Against Cyberattacks*, USA TODAY, June 15, 2007, at 20A; Landler & Markoff, *supra* note 2; *Newly Nasty, supra* note 5; Rodriguez, *supra* note 1.

forms of communication.[29] IO conceives of both information systems and information itself as new tools and new objectives for military activities. Unlike the expansion of criminal law to include cybercrimes, however, the law of war has gone unchanged. Therefore, the first question for future conflicts is whether the law of war covers IO at all. More importantly, even if the law of war does regulate IO, we need to ask whether it does so appropriately.

This Article explores the applicability and appropriateness of regulating IO under existing international legal frameworks. I find that the law of war currently governs IO, but only by analogy and then often in a patchwork fashion. Most states appear content with this situation, denying any need to develop an IO-specific legal framework. In doing so, however, states are doing themselves a great disservice. Even as it applies to IO, the existing system suffers from several, near-fatal conditions: *uncertainty* (i.e., states lack a clear picture of how to translate existing rules into the IO environment); *complexity* (i.e., overlapping legal regimes threaten to overwhelm state decision makers seeking to apply IO); and *insufficiency* (i.e., the existing rules fail to address the basic challenges of modern conflicts with non-state actors and to facilitate IO in appropriate circumstances). To redress these deficiencies, I propose that states adopt a new set of rules—an international law for information operations, or "ILIO."

Part II of this Article explores the meaning of the IO concept both in terms of its goals and the methods it employs. Part III argues that, notwithstanding any novelty of IO's goals or methods, the law of war does apply, albeit by analogy, and surveys the conventional wisdom favoring that status quo. Part IV challenges this conventional wisdom by analyzing the uncertainty created in analogizing existing rules to IO—such as those prohibiting the use of force, requiring civilian distinction, or banning perfidy. It questions the sufficiency of these rules to address the threats posed by non-state actors, particularly global terrorists. In addition, this part demonstrates the complexity of the status quo, given the multiple, overlapping legal regimes applicable to IO. Part V explains how a new set of rules, an ILIO, could remedy these problems while also serving a facilitative function that would allow the use of IO in appropriate circumstances in lieu of more traditional forms of force. The Article concludes by calling on states to draft an ILIO and explores some of the regulatory design questions that will undoubtedly accompany that exercise. In the end, this Article does not aim to offer any specific content for an ILIO, but rather seeks to address the threshold question of why states need an ILIO in the first place.

[29] *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 890 (1999).

II. UNDERSTANDING INFORMATION OPERATIONS

Computers and computer networks have become increasingly integral to government, military, and civilian functions. They allow instant communication and provide platforms on which business and government alike can operate. Computers now control both military and civilian infrastructures, including nuclear arsenals, telecommunication networks, electrical power systems, water supplies, oil storage facilities, banking and financial systems, and emergency services.[30] Other information networks—e.g., satellite and wireless telecommunication systems—play similar roles in facilitating the communication or distribution of information.

IO views these information networks as both new weapons for use in conflict and new targets for attack. IO aims to affect and protect computers and other communication systems, the data they contain, and the infrastructure they support.[31] The U.S. military defines IO broadly as seeking "to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting [one's] own."[32] IO employs various methods to achieve these objectives. Some of these methods have antecedents that date back to the beginning of warfare. Thus, IO extends the use of information technology and networks to "psychological operations" (psyops) that convey information (e.g., broadcasting satellite radio messages) with the aim of manipulating the views of foreign governments, organizations, or individuals.[33] Other IO methods have

[30] *See, e.g.*, Rho, *supra* note 12, at 700.

[31] *See* Schmitt, *supra* note 29, at 891 (IO's "defining aspect is that it operates on data existing in computers or computer networks").

[32] JOINT CHIEFS OF STAFF, U.S. DEP'T OF DEF., JOINT PUB. 3-13, INFORMATION OPERATIONS, at ix (2006), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf [hereinafter JP 3-13] (listing five IO methods: (1) electronic warfare; (2) computer network operations, including computer network attacks; (3) psychological operations; (4) military deception; and (5) operational security).

[33] *Id.* at II-1 (defining psyops as "planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals"). Other older methods adapted to the information context include military deception and operational security. Military deception uses information technology and computer networks to "deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations," so the adversary acts in ways that contribute to the friendly forces' mission. *Id.* at II-2. Operational security requires assessing critical information with an eye to deciding what information to convey to the adversary about friendly forces and intentions and what information to keep secure. *See id.* at II-3. Notwithstanding the apparent breadth of the U.S. IO definition, I regard IO that does not involve the use or targeting of information networks as falling outside the activities covered by IO and subject to regulation under existing international law. *Accord* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INT'L REV. RED CROSS 365, 365 (2002), *available at* http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/

more modern origins. For example, IO incorporates "electronic warfare"—i.e., using electromagnetic and directed energy to control or attack the adversary's electromagnetic spectrum (e.g., disabling systems that require electricity to operate).[34]

Much IO, however, centers on employing computers themselves in previously unavailable methods through the concept of "computer network operations" (CNO). CNO incorporates an offensive and a defensive element: (i) "computer network attacks" (CNA) that use data streams to deceive, disable, degrade, or destroy adversary computer systems or the infrastructure they support, and (ii) "computer network defense" that defends against an adversary's CNA.[35]

CNA in particular offers a wide spectrum of new opportunities for affecting an adversary. It might simply seek, as with Estonia, to deny access to information networks by flooding them with data requests.[36] In other instances, CNA could access adversary networks to acquire information, spread misinformation, or introduce weaknesses into the system (e.g., logic bombs that do no immediate harm, but have the potential to cause future injury when triggered by a specified time or event).[37] At its most potent, CNA involves taking control over adversary computer networks for the purposes of disabling them (temporarily or permanently) or affecting the infrastructure they support.[38] As the Estonia case demonstrates, moreover, the actor(s) committing CNA can remain anonymous or even disguise an attack's origins to appear as if it

5c5d5c?opendocument [hereinafter Schmitt II] (defining IO in terms of "data stored in a computer, manipulated by a computer or transmitted through a computer").

[34] JP 3-13, *supra* note 32, at II-4.

[35] *Id.* at II-4 to II-5 (defining CNO as the use of data streams to "attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure"). Of course, computers by themselves are incapable of serving as a weapon; to have that capacity, they require the additional elements of computer code and a code operator. *See* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 185 (2006).

[36] In lieu of denying access, CNA could simply delay access. Schmitt II, *supra* note 33, at 367 n.5. In addition to the Estonia example, hackers temporarily overwhelmed three of the thirteen computers that provide the platform for the entire Internet in February of 2007. *See* Ted Bridis, *Hackers Attack Key Net Traffic Computers*, ASSOCIATED PRESS, Feb. 7, 2007.

[37] Schmitt, *supra* note 29, at 892; Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STAN. J. INT'L L. 207, 208 n.2 (2002) (discussing various CNA operations).

[38] Acquiring control over adversary computer networks can occur through various hacking tools, including viruses, worms, and Trojan horses. Viruses are fragments of code that attach themselves to other computer instructions and, when their host program begins to run, execute payloads that can do anything from displaying messages to deleting files. Worms are programs that independently propagate themselves from one computer to another over a network, breaking in much the same way that a hacker would. Trojan horses are programs that disguise viruses and worms to allow attackers to gain access to systems. *See* Barkham, *supra* note 12, at 62–63; Jensen, *supra* note 37, at 208 n.2; Schmitt II, *supra* note 33, at 367 n.5.

comes from some other identifiable source.[39] In other situations, CNA may occur surreptitiously, such that the victim has no knowledge of an attack, or it replicates effects that could have innocent sources such as computer error or malfunction.[40]

Thus, CNA specifically (and IO generally) has the potential to do through the transmittal of data streams what militaries have previously done with bombs and missiles (i.e., depriving the adversary of infrastructure that supports military operations such as electrical or communication systems). But IO also offers the promise of accomplishing such goals without as much collateral damage—e.g., disabling an electrical grid temporarily through CNA in lieu of destroying the power plant that produces the electricity, or using electronic warfare to disable broadcasting communications in lieu of bombing the facilities and causing some collateral loss of life. Moreover, IO methods such as psyops present alternative ways to accomplish larger strategic goals without resorting to force at all by convincing the adversary (or those who support it) to change their policies or positions. In this sense, IO may target more than an adversary's military, including other government agencies, political elites, or the populace as a whole. IO presents new means for states to reach and affect non-state actors, and, of course, affords non-state actors new means for reaching and affecting nation-states.

IO's broad aims and wide array of methods have led many scholars to try to narrow its scope, focusing alternatively on just its offensive capabilities, its use in international armed conflicts, or its use exclusively by nation-states.[41] Although such scholarship has undoubted value, it may actually define away some of the aspects of IO that most warrant legal attention. For example, to focus only on IO's offensive use excludes the important questions surrounding what authorities (or limits) exist for governments and their militaries in responding to and defending against an IO attack.[42] Similarly, to examine IO only in an international armed conflict between states ignores its use between states in cases falling short of an armed conflict (of which Estonia might be an example, *if* Russia

[39] Schmitt, *supra* note 29, at 892 (describing how the identity of an attacker can be "spoofed . . . to convince the victim that the attack originated elsewhere").

[40] Jensen, *supra* note 37, at 212–13; Barkham, *supra* note 12, at 64.

[41] *See, e.g.*, Brown, *supra* note 35, at 185–87 (noting difficulties in IO-related terminology and devising term "information attack" to cover only offensive uses of computers as weapons); Schmitt II, *supra* note 33, at 367–68 (addressing use of CNA during international armed conflicts between states and focusing on what the law of war allows states to do during such hostilities); Schmitt, *supra* note 29, at 891 (distinguishing IO from "information warfare" that refers to IO conducted during times of crisis or conflict, and not during peacetime); Rho, *supra* note 12, at 701–02 (considering computer attack committed by private entity to not qualify as IO, but instead as cybercrime, governed by the domestic law of the relevant state).

[42] *See infra* notes 111–17, and accompanying text (discussing problems under existing international law for states seeking to respond to an IO attack).

indeed played a role) or IO's usage by states in non-international struggles, such as the Israeli-Palestinian conflict or civil wars.[43]

Even as the Estonia case opens up the possibility that IO will create new battlefields for state-to-state conflicts, it would be dangerous to focus only on such IO to the exclusion of IO attacks by (or against) non-state actors.[44] The nature, costs, and availability of computers, computer networks, and other information technology provide non-state actors, including those bent on global terror, with the capacity to conduct IO in many ways analogous to its potential use by states.[45] Finally, notwithstanding the theoretical simplicity accompanying narrower IO definitions, the reality is that states have begun to organize their militaries around the IO concept, devising strategic, operational, and tactical doctrines for IO. In addition to the United States, more than thirty other states—including China, India, and Russia—have reportedly begun to develop IO doctrines or capabilities.[46] Thus, a broad definition of IO—i.e., the use of information technology to affect or protect information or information networks—serves as the best starting point for considering the application of existing international law and any need for new IO-specific rules.

III. THE EXISTING IO REGIME—INTERNATIONAL LAW BY ANALOGY

Since its inception, the modern law of war has sought to restrict the aim of warfare to the achievement of military objectives. In the first treaty

---

[43] Israeli websites in particular have come under frequent attack by Palestinians or those sympathetic to their cause. Landler & Markoff, *supra* note 2. For example, in 2006, as Israel conducted military operations in Gaza, over 750 websites came under attack from a Moroccan group of hackers dubbed "Team Evil." They targeted Israeli banks, hospitals, and various Israeli corporations, causing damage to the sites and posting messages on them that said: "You're killing Palestinians, we're killing servers." Gal Mor & Ehud Kinan, *Major Israeli Websites Hacked*, YNET ISRAEL NEWS, June 28, 2006, http://www.ynetnews.com/articles/0,7340,L-3268449,00.html.

[44] *See, e.g.*, Jensen, *supra* note 37, at 213 ("the threat from subgroups and terrorist organizations is very real" with goals of using IO for purposes of "disruption, intimidation, or publication of a political message").

[45] Other non-state actors may have different aims, whether it is a teenage hacker seeking the thrill of an attack against a government computer network or a criminal organization seeking to extort money from a company or industry by threatening or using IO-like methods. *See* Condron, *supra* note 12, at 411. Although these activities may qualify as IO, any ILIO that states adopt will need to consider whether there remain better remedies under a criminal law model that operates in concert with these new rules or if they warrant actual integration into a single set of rules for all IO, regardless of its source.

[46] *See* MAX BOOT, WAR MADE NEW 448 (2006); Condron, *supra* note 12, at 405 (describing China's integration of "information warfare units" into its military operations with first strike capabilities); John Lasker, *U.S. Military's Elite Hacker Crew,* WIRED, April 18, 2005, http://www.wired.com/politics/security/news/2005/04/67233 (describing U.S. military's formation of a "Joint Functional Component Command for Network Warfare"); Jensen, *supra* note 37, at 212.

prohibiting a weapon of war—the 1868 St. Petersburg Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight—the parties agreed that "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy."[47] IO's goals, in contrast, are different—they can focus on affecting the entire adversary (e.g., the government and political elites), not just its military force. Although IO might seek to produce physical damage akin to classic applications of kinetic force, its purpose will more often center on affecting information or information systems held by the adversary. On the surface, the differing goals of IO and more traditional warfare suggest a possible reason to give IO different rules than those normally applied under the law of war.[48]

But, it would be a mistake to justify ILIO on such grounds. In reality, the goal of warfare has always involved more than just inflicting physical damage or destruction upon an enemy's military forces. States have long employed the methods of war to control or convey information to belligerents, which can then compel them towards a desired outcome. Thucydides' account of the Melian Dialogue portrays Athens' justification for its eventual slaughter of hostile Melian islanders purely in terms of the information that it will communicate to other states about Athens' claims to dominance. Rejecting Melian pleas for neutrality, the Athenians contended:

> [I]t is not so much your hostility that injures us; it is rather the case that, if we were on friendly terms with you, our subjects would regard that as a sign of weakness in us . . . . [B]y conquering you we shall increase not only the size but the security of our empire. We rule the sea and you are islanders, and weaker islanders too than the others; it is therefore particularly important that you should not escape.[49]

Nor is this idea of "war as message" an entirely Western invention. Sun Tzu gauged the ultimate military objective as lying well beyond the battlefield and the defeat of enemy forces: "to win a hundred victories in a hundred battles is not the highest excellence; the highest excellence is

---

[47] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Dec. 11, 1868, *available at* http://www.icrc.org/ihl.nsf/FULL/130?Open Document. The United States did not join the Declaration, which has twenty state parties. *See id.*

[48] Alternatively, the St. Petersburg formulation might operate to limit IO to the traditional objectives of war, or even to prohibit it entirely insofar as IO's objectives avowedly differ from that formulation.

[49] THUCYDIDES, HISTORY OF THE PELOPONNESIAN WAR, Book V, ¶¶ 95, 97, at 402–03 (Rex Warner trans., Penguin Books 1972) (n.d.). For their part, the Melians argued Athenian conquest would send a different message: "Is it not certain that you will make enemies of all states who are at present neutral, when they see what is happening here and naturally conclude that in course of time you will attack them too?" *Id.* ¶ 98, at 403.

to subdue the enemy's army without fighting at all."[50] IO often aims to accomplish just that, seeking to affect information held by the adversary under the belief that such effects, in turn, can avoid or end conflicts. In attempting to affect information and information networks, moreover, IO's goals ultimately have a political character that aspires to reach beyond the military battlespace. As Clausewitz reminds us, however, such objectives are at the core of all methods of warfare: "[W]ar is not a mere act of policy but a true political instrument, a continuation of political activity by other means . . . . The political object is the goal, war is the means of reaching it, and means can never be considered in isolation from their purpose."[51]

Even if IO's objectives do not place it beyond the reach of existing international law, perhaps the tools employed in IO do. CNA, for example, provides a new weapon that can be deployed instantaneously and surreptitiously thousands of miles away from its target. Although its effects can certainly cause death and destruction (e.g., unleashing a computer virus on a nuclear power plant's operating system), CNA also has the potential to avoid, or at least minimize, such effects (e.g., disabling or usurping adversarial information systems temporarily). Such a military capacity was never foreseen by states in developing the existing law of war. As a result, at present, the law of war includes *no* provisions specifically addressing IO. This raises the possibility that IO could escape existing international law through the application of the *Lotus* principle—i.e., what international law does not prohibit, it permits.[52]

As with arguments differentiating IO's objectives, however, exceptional arguments about IO methods cannot succeed. The Permanent International Court of Justice applied the *Lotus* principle in one specific context—where a state sought to apply its criminal laws beyond its borders—and states have explicitly declined to extend *Lotus* to the law of war. On the contrary, pursuant to the "Martens Clause," the absence of a treaty provision explicitly prohibiting conduct during armed conflict does not mean that international law permits it.[53] The modern

[50] SUN TZU, THE ART OF WARFARE 111 (Robert G. Henricks ed., Roger T. Ames trans., Ballantine Books 1993) ("the expert in using the military subdues the enemy's forces without going to battle, takes the enemy's walled cities without launching an attack, and crushes the enemy's state without a protracted war").

[51] CARL VON CLAUSEWITZ, ON WAR 87 (Michael Howard & Peter Paret eds. & trans., 1976).

[52] In the *Lotus* case, the Permanent International Court of Justice endorsed this principle and rejected the reverse presumption that states need to establish the existence of an authorizing international law rule in order to act. *See* S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18–19 (Sept. 7) (Given the "very nature and existing conditions of international law . . . [r]estrictions upon the independence of States cannot therefore be presumed" and "all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction.").

[53] The clause, named after famed Russian international lawyer, Friedrich Martens, first appeared in the preamble to Hague Convention II with Respect to the Laws and Customs of War on Land of 1899. It has continued to appear in subsequent

version of the clause, found in Additional Protocol I to the 1949 Geneva Conventions, indicates where treaties are silent "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."[54] In other words, the law of war governs IO even without mentioning it specifically.[55]

Nor does the novelty of CNA or other technological innovations of IO preclude application of the law of war or legal restrictions on the use of force. States have a history of subjecting "novel" developments in warfare—e.g., submarines and airpower, as well as nuclear, chemical, and biological weapons—to legal regulation. In its advisory opinion, *Legality of the Threat or Use of Nuclear Weapons*, the International Court of Justice (ICJ) had "[n]o doubt as to the applicability" of international law, reasoning that any threat or use of nuclear weapons must comply with "the international law applicable in armed conflict, particularly those of the principles and rules of international humanitarian law."[56] Moreover, the law of war now explicitly applies to novel developments. Article 36 of Additional Protocol I records the affirmative duty of states that develop or acquire "a new weapon, means or method of warfare . . . to determine whether its employment would, in some or all circumstances, be

international humanitarian law agreements, including the 1949 Geneva Conventions. *See, e.g.*, Hague Convention (IV) Respecting the Laws and Customs of War on Land, Preamble, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631; Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 63, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 62, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; Geneva Convention Relative to the Treatment of Prisoners of War art. 142, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 158, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV] [collectively hereinafter, Geneva Conventions].

[54] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1), art. 1.2, *adopted* June 8, 1977, 1125 U.N.T.S. 3, *available at* http://www.ohchr.org/english/law/protocol1.htm [hereinafter AP I]; *see also id.*, art. 35.1. Although not a party, the United States considers many of Additional Protocol I's provisions declaratory of customary international law. *See, e.g.,* Michael J. Matheson*, Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419, 420 (1987).

[55] *See also* AP I, *supra* note 54, art. 35.1 ("[T]he right of the Parties to the conflict to choose methods or means of warfare is not unlimited.").

[56] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 35 I.L.M. 809, ¶¶ 85, 105(2)(D) (July 8, 1996). By a narrow margin, the ICJ also found that although the threat or use of nuclear weapons would "generally" violate the law of armed conflict, it could not "conclude definitively whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defence, in which the very survival of a State would be at stake." *Id.* ¶ 105(2)(E).

prohibited by this Protocol or by any other rule of international law applicable."[57] Thus, IO cannot escape a law of war analysis.[58]

To say the law of war covers IO does not, of course, tell us *when* and *how* it applies. States have historically accommodated changes in weapons, tactics, and new types of conflict in one of three ways. First, as Article 36 of Additional Protocol I suggests, states frequently extend the existing rules to new types of warfare by analogy; for example, the rules of air warfare derived largely from the rules for land warfare.[59] Second, states develop specific rules regulating—or even prohibiting—particular weapons or their deployment, such as the treaties on biological and chemical weapons.[60] Third, states periodically seek to update and revise the law of war, usually in reaction to recent experience; the Additional Protocols to the 1949 Geneva Conventions represent the most recent iteration of that phenomenon.[61] At present, there are no specific rules for IO, nor is there any sign of a more general revision to accommodate IO. Thus, IO falls under the first approach—the law of war governs IO by analogy.

Conventional wisdom suggests that IO can be effectively governed by the analogy approach. In 1998, states were unresponsive to Russia's request that states devise new international law rules to prohibit particularly dangerous information weapons.[62] The U.S. Department of

[57] AP I, *supra* note 54, art. 36.

[58] *See* Louise Doswald-Beck, *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, 76 INT'L L. STUD. 163, 164 (2002) ("It is perfectly reasonable to assume that CNA is subject to [international humanitarian law] just as any new weapon or delivery system has been so far when used in an armed conflict.").

[59] *See* Hague Convention (IV) Respecting the Laws and Customs of War on Land, *supra* note 53.

[60] *See* Protocol for Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, *done* June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, 32 I.L.M. 800.

[61] *See* AP I, *supra* note 54; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), *adopted* June 8, 1977, 1125 U.N.T.S. 609, *available at* http://www.ohchr.org/english/law/pdf/protocol2.pdf [hereinafter AP II]. The 1949 Geneva Conventions in turn reflected an attempt to elaborate and develop the 1929 Geneva Conventions and Hague Convention (X) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention.

[62] *See* Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General, U.N. GAOR, 53d Sess., U.N. Doc. A/C.1/53/3(1998), *available at* http://daccessdds.un.org/doc/UNDOC/GEN/N98/284/58/PDF/N9828458.pdf; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/54/213 (Aug. 10, 1999) (of nine states submitting views, only Cuba and Belarus favored negotiations to restrict information warfare). Ultimately, the U.N. General Assembly passed Resolution 53/70, calling on

Defense Office of General Counsel has since rejected calls for IO-specific rules as "premature," arguing, for example, that in regulating IO via the law of war, the "process of extrapolation appears to be reasonably predictable."[63] More generally, the International Committee for the Red Cross (ICRC) opined in 2003 that "the existing legal framework is on the whole adequate to deal with present day international armed conflicts."[64] A majority of military thinkers agree, arguing in favor of an analogy approach or decrying the possibility of IO-specific rules as premature or unrealistic.[65]

Member States simply to promote consideration of existing and potential threats to information security. U.N. GAOR, 53d Sess., 79th plen. mtg. at 1, U.N. Doc. A/RES/53/70 (Jan. 4, 1999).

[63] Office of Gen. Counsel, Dep't of Def., *An Assessment of International Legal Issues in Information Operations* (Nov. 1999), *reprinted in* 76 INT'L L. STUD. 459, 475, 520 (2002), *available at* http://www.nwc.navy.mil/cnws/ild/studiesseries.aspx (follow "volume 76" hyperlink) [hereinafter *DOD GC Memo*]; *id.* at 522 ("There seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most of the areas of international law that are directly relevant to information operations.").

[64] INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 4 (2003), *available at* http://www.icrc.org/web/eng/sisteeng).nsf/htmlall/5XRDCC/$File/IHLContemp_armedconflicts_FINAL_ANG.pdf; Sean Watts, Civilian Participation in Computer Network Attacks 32 (draft manuscript, dated 2006, on file with author).

[65] *See, e.g.*, Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1149 (2003) [hereinafter Jensen II] (rejecting proposals for new agreements on CNA as "unnecessary" where commanders can "apply the traditional analysis . . . to ensure that they correctly apply this new technology during armed conflict"); Schmitt II, *supra* note 33, at 396 (although it poses some new and sometimes troublesome quandaries, "[b]y and large, existing humanitarian prescriptive norms suffice"). The consensus at a 1999 Naval War College conference disfavored CNA-specific rules with respect to information warfare. Philip A. Johnson, *Is it Time for a Treaty on Information Warfare?*, 76 INT'L L. STUD. 439, 439 (2002). Many took the view that the law of war could operate by analogy. *See, e.g.*, Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 114–15 (2002) ("no insuperable difficulty in applying the general principles and rules of international law to the novel weapon (subject to some adjustments and adaptations, which crystallize in practice)"); Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, 76 INT'L L. STUD. 73, 75 (2002) (absent consensus on status of CNA under U.N. Charter, argues we "must proceed on the basis of analogy to such possibly relevant authority and doctrine as exists in other contexts"); Douglas S. Anderson & Christopher R. Dooley, *Information Operations in the Space Law Arena: Science Fiction Becomes Reality*, 76 INT'L L. STUD. 265, 298 (2002) (suggesting states "resist the temptation of expecting that these apparent futuristic tools require a whole new set of laws" in favor of applying "old laws and principles to new military scenarios"). Others characterized the idea as premature or unlikely. Arthur K. Cebrowski, *CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers,* 76 INT'L L. STUD. 1, 6 (2002) ("We must be cautious not to advocate new law regarding information warfare without understanding its moral, legal, and practical implications."); Charles J. Dunlap, Jr., *Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy*, 76 INT'L L. STUD. 353, 362–63 (2002) ("we ought to be cautious about entering into legal regimes that may unnecessarily hamper what is, after all, an area

IV. THE NEED FOR AN INTERNATIONAL LAW FOR INFORMATION OPERATIONS (ILIO)

A closer examination of the IO law-by-analogy approach reveals four substantial flaws in the conventional wisdom. First, even in the context of armed conflict, there are serious "translation" problems with extending the existing rules to IO. Such translation problems produce uncertainty, creating conflicting views of what the law requires as well as disincentives to engage in IO that might cause less harm than traditional kinetic weaponry. Second, the vast majority of IO scholarship has focused on regulating IO's application to international armed conflicts involving two or more nation-states. But such analyses are clearly insufficient. They ignore the new reality of asymmetrical conflict that increasingly pits states—not against each other—but against non-state actors. Third, any consideration of IO beyond the *lex specialis* applicable to the law of war immediately encounters nearly incoherent complexity. IO finds itself subject to multiple legal regimes—some overlapping, others applying in the alternative—depending on the context. Such complexity undoubtedly further clouds the minds of military commanders asked to employ or defend against IO. Fourth, the current rules operate almost exclusively in a restrictive fashion, limiting when and how states employ IO. In doing so, the current regime fails to acknowledge—let alone encourage—the functional benefits IO can achieve in both traditional and asymmetrical conflicts.

By adopting ILIO, states could alleviate all of these problems. Military commanders would benefit from a new *lex specialis*, a single set of IO-related rules, especially if the rules covered the entire range of circumstances in which militaries might employ IO. At the same time, ILIO offers the possibility of lessening the collateral costs of armed conflicts while improving the relative position of states in their fight against global terror.

A. Translation Problems

Hundreds of rules govern when states can use force (the *jus ad bellum*) and how they can use that force in an armed conflict (the *jus in bello* or "law of war"). These rules have diverse sources, including the U.N. Charter, international humanitarian law treaties (e.g., the 1949 Geneva Conventions), as well as customary international humanitarian law. Some of this existing law has little to say about IO specifically (e.g., the protections owed the wounded, sick, or shipwrecked). Others involve principles of general applicability that presumably encompass IO, such as

where the US, as the world's foremost digital power, may itself have an asymmetric advantage"); David Tubbs, Perry G. Luzwick & Walter Gary Sharp, Sr., *Technology and Law: The Evolution of Digital Warfare,* 76 INT'L L. STUD. 7, 17 (2002) (comprehensive regulation of CNA "unlikely").

those regulating the use of force, distinction, military necessity, proportionality, and perfidy. Nevertheless, the gap between physical weaponry (whether kinetic, biological, or chemical) and IO's virtual methods can be substantial, creating acute translation problems. Attempts to apply existing principles to IO result either in no clear rules emerging or a rule that contravenes other principles fundamental to the law of war. Three examples illuminate the nature and scope of the problem: (1) the prohibition on the use of force; (2) the requirement of civilian distinction; and (3) the ban on perfidy.[66]

1. The Prohibition on the Use of Force

The U.N. Charter prohibits states from the threat or use of force, except when authorized by the U.N. Security Council or pursuant to the inherent right of self-defense in response to an armed attack.[67] Historically, states defined "force" in terms of the instrument used, including "armed" force within the prohibition, but excluding economic and political forms of coercion.[68] Although not without controversy, this distinction reflects an effort to proscribe those acts most likely to interfere with the U.N.'s primary purpose—maintaining international peace and security.[69]

The use of force prohibition encounters real difficulty, however, when translated into the IO context. Commentators have "come to widely divergent conclusions," such that no bright line rule exists for when IO constitutes a use of force, let alone an armed attack for self-

[66] Nor do these constitute the only translation problems for the law of war's application to IO; we could just as easily discuss the difficulties posed in trying to apply the law of neutrality to IO. *See, e.g.*, Doswald-Beck, *supra* note 58, at 173; George K. Walker, *Neutrality and Information Warfare*, 76 INT'L L. STUD. 233 (2002) (analogizing neutrality rules for land, air and sea to IO).

[67] U.N. Charter, art. 2, para. 4 & arts. 42, 51. Despite the prohibition's linkage to threats or uses of force against a state's "territorial integrity or political independence," state practice has interpreted the prohibition more broadly to extend to all threats and uses of force. *See, e.g.*, Schmitt, *supra* note 29, at 901. Moreover, the International Law Commission characterized the prohibition as *jus cogens,* a preemptory norm of international law. *See* International Law Commission, *Report of the International Law Commission on the Work of its Eighteenth Session*, 247, U.N. Doc. A/CN.4/191 (July 19, 1966), *available at* http://www.un.org/law/ilc/index.htm (follow "Search" hyperlink; then enter U.N. Doc. number).

[68] Schmitt, *supra* note 29, at 905; Horace B. Robertson, Jr., *Self-Defense Against Computer Network Attack Under International Law,* 76 INT'L L. STUD. 121, 134 (2002).

[69] Indeed, those who favor the prohibition's application to threats and use of economic and political force can argue that a limited border incursion, while violating the prohibition, really poses less a risk to international peace and security than a major economic embargo. *See* Schmitt, *supra* note 29, at 909. But, as Michael Schmitt explains, armed force can produce immediately apparent consequences in terms of human casualties and property destruction that risk further escalation, whereas economic or political coercion are unlikely to produce comparable effects, and when they do, they are unlikely to occur with the immediacy or direct causality attributable to kinetic weaponry. *Id.* at 912.

defense purposes.[70] Three different possibilities remain in play. First, the classic "instrumentality" approach argues IO does not qualify as armed force because it lacks the physical characteristics traditionally associated with military coercion.[71] The text of the U.N. Charter offers some support for this view; Article 41 lists "measures not involving the use of armed force" to include "complete or partial interruption of . . . telegraphic, radio, and other means of communication."[72] Second, the "target-based" approach suggests IO constitutes a use of force or an armed attack whenever it penetrates "critical national infrastructure" systems, even absent significant destruction or casualties.[73] Third, the "consequentiality" approach, favored by the U.S. Department of Defense, focuses on IO's consequences; whenever IO intends to cause effects equivalent to those produced by kinetic force (death or destruction of property), it constitutes a use of force and an armed attack.[74]

The problem, however, goes beyond picking a definitional standard. Absent further elaboration, the novelty of IO methods generates confusion regardless of the standard chosen.[75] Each approach proves

[70] *See* Silver, *supra* note 65, at 75, 86 (discussing CNA and the prohibition on the use of force); Emily Haslam, *Information Warfare: Technological Changes and International Law*, 5 J. CONFLICT & SEC. L. 157, 165 (2000) (use of force paradigm applies "only with difficulty"); *DOD GC Memo*, *supra* note 63, at 491 ("It is far from clear the extent to which the world community will regard computer network attacks as 'armed attacks' or 'uses of force.'"); *cf.* Brown, *supra* note 35, at 181 n.12 (concluding that a "*jus ad bellum* of information warfare can be derived with little difficulty").

[71] Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 288–89 (1996); David DiCenso, *Information Operations: An Act of War?*, AIR & SPACE POWER CHRONICLES (July 2000), *available at* http://www.airpower.maxwell.af.mil/airchronicles/cc.html.

[72] U.N. Charter, art. 41. Since "means of communication" would include not only interpersonal communication (e.g., on the Internet) but how an operating system communicates with the infrastructure it controls, almost all CNA could qualify as targeting "means of communication."

[73] *See, e.g.*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129–32 (1999); Jensen, *supra* note 37, at 229; Condron, *supra* note 12, at 415–16. For those who favor a target-based approach, the interpretative exercise largely focuses on determining when a state may respond to CNA in self-defense, including the right of anticipatory self-defense.

[74] *DOD GC Memo*, *supra* note 63, at 483; Silver, *supra* note 65, at 85; Dinstein, *supra* note 65, at 105; Robertson, *supra* note 68, at 133; *see also* Schmitt, *supra* note 29, at 913, 919 (admitting that a consequential interpretation of Article 2(4) requires a "radical teleological interpretation"). Not all uses of force will constitute an "armed attack"—bullets fired across a border may be a use of force, but not an armed attack for purposes of triggering self-defense. Dinstein, *supra* note 65, at 100.

[75] Of course, the U.N. Charter also prohibits the "threat" of a use of force, which may involve an entirely separate line of inquiry in the IO context. U.N. Charter, art. 2, para. 4. For example, even if IO doesn't produce consequences akin to classic armed force, it may be employed as a prelude to an attack without itself causing any destruction or casualties. Can states respond in self-defense even in the absence of a traditional armed attack? Like the use of force definition more generally, the IO context has yet to produce any clear answers.

inadequate in the modern context. Under the instrumentality approach, for example, the prohibition on the use of force would not restrict IO against communication systems. But does that mean IO shutting down an entire civilian air traffic communication system—downing airliners and causing significant casualties—does not qualify as a use of force or give rise to a right of self defense?[76] In contrast, the target-based approach might suffer from over-inclusion. IO can produce wide-ranging effects, from merely informational (distributing propaganda) to inconvenient (disrupting systems temporarily via a denial-of-service attack) to potentially dangerous (implanting a logic bomb doing no immediate harm but with the potential to cause future injury) to immediately destructive (disabling a system permanently via a virus). Does the target's identity as somehow "critical" alone qualify such divergent acts as uses of force or armed attacks? Finally, even as the consequences approach covers IO effects that replicate kinetic force, it leaves unregulated the very aspects of IO that make it so novel. Neither kinetic force nor political or economic sanctions can disable an entire stock market or banking system the way IO can—immediately and without casualties or physical destruction. Do we treat IO as outside the U.N. Charter whenever its effects differ from kinetic force? Or, do we include it under the prohibition where its effects have an immediacy not seen in economic or political coercion that may generate more civil disturbances or disruption?[77]

2. The Requirement of Civilian Distinction

Irrespective of how it commences, once states engage in armed conflict, the law of war (or the *jus in bello)* applies. Among that law's core principles is the requirement of civilian distinction; i.e., that conflicting states "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."[78] Thus, militaries can only "attack" military objectives, "which

[76] In raising this possibility, I do not mean to suggest the downing of any civilian aircraft would otherwise qualify as a prohibited use of force. States did not regard the Lockerbie incident as such, using a criminal law approach instead to try the two accused Libyan intelligence agents for their role in downing Pan Am Flight 103. At the same time, however, the possibility of IO accomplishing results akin to that tragedy are not entirely theoretical. In 1997, a Massachusetts hacker shut down all communications to a Federal Aviation Administration control tower at an airport for over six hours. Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 389 (2007).

[77] Silver suggests that CNA producing effects that are only of an economic or political nature do not violate the Charter's use of force restrictions, even if they "crippled the financial infrastructure of a target State" and "[e]ven if angry investors rioted and tore down the stock exchange." Silver, *supra* note 65, at 85.

[78] AP I, *supra* note 54, art. 48. Other *jus in bello* principles may also require translation into the IO context, e.g., rules on indiscriminate weapons and proportionality. *See, e.g., id.* art. 51(4)–(5); Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks* (Nov. 19, 2004), http://www.icrc.org/

by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[79] All other objects are deemed civilian and off-limits (as are civilians themselves unless taking a direct part in the hostilities).[80] Application of this principle has proved difficult even in traditional international armed conflicts—witness questions about whether Serbian television stations or Baghdad's electrical power system constituted proper military objectives.[81] The IO context, however, exacerbates existing confusion and, indeed, may actually undermine the concept of civilian distinction entirely.

Among IO's most significant challenges to the principle of civilian distinction is confusion surrounding (i) what IO triggers the civilian distinction requirement; and (ii) the dual-use nature of most information infrastructure.[82] Generally, civilian distinction does not protect civilians and their objects from all military operations, only those that qualify as "attacks," defined as "violence against the adversary, whether in offence or in defence."[83] As in the use-of-force context, much depends on which IO qualifies as an "attack." IO that results in casualties or physical destruction likely qualifies as an "attack." Other effects remain open to debate (e.g., neutralizing a target, denying service to a system), or clearly fall outside the definition (e.g., psyops, electronic embargoes). The irony of IO is that the less likely it is that a particular IO functions as an attack, the more likely it is that its use against civilians and their objects is permissible. In other words, IO's development may actually result in warfare having more impact on civilians by expanding militaries' ability to target (but not attack) them. In such circumstances, applying existing civilian distinction rules to IO challenges the notion that the law of war should protect civilians and their property as much as possible.[84] On the

Web/Eng/siteeng0.nsf/html/68LG92; Doswald-Beck, *supra* note 58, at 168–69; Jensen II, *supra* note 65, at 1177–79; Schmitt II, *supra* note 33, at 389–90.

[79] AP I, *supra* note 54, art. 52(2).

[80] *Id.* arts. 51(2), 52(1). In addition, international humanitarian law also provides special protection to certain objects (e.g., medical facilities, objects indispensable to the survival of the civilian population including drinking water, foodstuffs, etc.). *See* Dörmann, *supra* note 78, at 6–8.

[81] *See DOD GC Memo*, *supra* note 63, at 471–72; Schmitt II, *supra* note 33, at 381–82; Haslam, *supra* note 70, § 4.3.2, at 172. Louise Doswald-Beck describes how the military objectives definition developed to avoid the slippery slope of World War II where attacks on "quasi-combatants" who aided in the "war effort" devolved into wholesale destruction of cities. Doswald-Beck, *supra* note 58, at 167.

[82] The status of civilians whom militaries employ to conduct IO raises its own set of translation questions. *See, e.g.*, Dörmann, *supra* note 78, at 8–9; *DOD GC Memo*, *supra* note 63, at 470–71; Schmitt II, *supra* note 33, at 383–84.

[83] AP I, *supra* note 54, art. 49(1). However, all "[a]cts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited." *Id.* art. 51(2).

[84] *See* Schmitt II, *supra* note 33, at 378–79; Haslam, *supra* note 70, § 4.3.2, at 173.

other hand, even if IO targets more civilians, by having more humane effects than traditional kinetic weapons we might accept an expansion of traditional targeting rules for IO.[85]

Restricting IO "attacks" to military objectives may also fail to protect civilians and their property. The law of war places on states a responsibility to separate "to the maximum extent feasible" civilian populations and objects from the vicinity of military objectives and dangers of military operations.[86] When they do not—i.e., where infrastructures have a "dual-use" serving both civilian and military purposes—they qualify as military objectives subject to attack, even if their primary purpose is not military, but civilian. If that rule holds for IO, however, then militaries may target virtually all computer networks. As of 2000, 95% of all U.S. military traffic moved over civilian telecommunication and computer systems, and the trend is clearly towards greater consolidation of civilian and military technology.[87] The dual-use rule suggests, therefore, that U.S. adversaries may treat all U.S. communication systems as military objectives and attack them by IO or kinetic means.[88] Thus, application of the civilian distinction principle to IO not only involves uncertainty, it also suggests increasing tension with the principle's purported goal of restricting military attention on civilians and their property as much as possible during conflict.

3. The Ban on Perfidy

The law of war prohibits perfidy—the killing, injuring, or capturing of adversaries by "[a]cts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence."[89] Perfidious acts include feigning surrender, civilian status, non-combatant status, or other "protected status" such as that of a neutral state. In contrast, ruses of war—acts that do not feign protected status but which seek to mislead adversaries and cause them to act recklessly—are permitted, including use of misinformation and decoys.[90]

IO presents a host of new opportunities for states to engage in both ruses and perfidy, since both ultimately turn on distributing (mis)information. The difficulty, however, lies in categorizing permitted and prohibited IO. Perfidy presently only applies if it results in injury to,

---

[85] *See* Jensen II, *supra* note 65, at 1166.

[86] AP I, *supra* note 54, art. 58.

[87] ARNAUD DE BORCHGRAVE ET AL., CTR. FOR STRATEGIC & INT'L STUD., CYBER THREATS AND INFORMATION SECURITY: MEETING THE 21ST CENTURY CHALLENGE (2001); Dörmann, *supra* note 78, at 10; *DOD GC Memo*, *supra* note 63, at 472.

[88] Doswald-Beck, *supra* note 58, at 167. Of course, as military objectives, they would remain subject to the rules on discrimination and proportionality that might limit how an adversary's military attacked them. *See* Schmitt II, *supra* note 33, at 385.

[89] AP I, *supra* note 54, art. 37(1).

[90] *Id.* art. 37(2).

or the capture of, adversaries.[91] As a result, it appears that IO otherwise feigning protected status (e.g., conducting CNA as if originating from a civilian source) does not constitute perfidy if it only produces physical damage but no casualties.[92] Would it make more sense to require all military IO to identify its origins?[93] Or, does an analogy to the rules regarding individuals feigning civilian status fall apart in the CNA context? After all, in many cases, IO will only deceive a computer system, not the individual adversary perfidy purports to protect. Of course, in other situations, the perfidy analogy may hold, as when a virus masks itself as coming from a civilian source (e.g., e-mail purportedly from a civilian family member of an individual adversary).[94] Additional confusion exists over the ability of IO to feign its origin as coming from the adversary, such as accessing an information network to alter enemy orders en route to enemy forces. If such IO equates to employing enemy watchwords or signal calls to mislead enemy forces, it likely constitutes a permissible ruse.[95] On the other hand, if we equate such IO to attacking the enemy while wearing the enemy's own uniform, it would constitute prohibited perfidy.[96]

Taken together, these examples illustrate the scope and depth of confusion that IO generates in the context of armed conflict. In all three instances—use of force, civilian distinction, and perfidy—the current rules do not translate easily or clearly into the IO context. All told, states are left without any real sense of what they can and cannot do in their IO. This leaves states and their militaries in a quandary. They can apply their own translation of the law of war and use of force prohibitions to IO and trust others will acquiesce. But foreign forces may not acquiesce. Indeed, they may adopt conflicting translations that produce

---

[91] Dörmann, *supra* note 78, at 11; Schmitt II, *supra* note 33, at 395.

[92] Regardless of perfidy, states may not falsely employ certain emblems or signals, such as those belonging to the ICRC or to medical transports and units. *See* AP I, *supra* note 54, art. 38; Dörmann, *supra* note 78, at 11.

[93] Jeffrey H. Smith & Gordon N. Lederman, *"Weapons Like to Lightning"—US Information Operations and US Treaty Obligations,* 76 INT'L L. STUD. 375, 388–89 (2002) (suggesting that the current law of perfidy requires identifying marks for military IO).

[94] Ruth G. Wedgwood, *Proportionality, Cyberwar, and the Law of War,* 76 INT'L L. STUD. 219, 227 (2002) (arguing that masking a state-sponsored attack as coming from a civilian source could be perfidy); Dörmann, *supra* note 78, at 11; Brian T. O'Donnell & James C. Kraska, *International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement*, 76 INT'L L. STUD. 395, 411 (2002) [hereinafter O'Donnell & Kraska] (noting differing views as to whether identifying a harmful e-mail's origin as from Microsoft would constitute perfidy).

[95] 2 LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE 429 (H. Lauterpacht ed., 7th ed. 1952) (1906) (including use of enemy watchwords, and mimicking enemy bugle calls and signals as acceptable military ruses); Doswald-Beck, *supra* note 58, at 171.

[96] AP I, *supra* note 54, art. 39; Dörmann, *supra* note 78, at 12 (noting conflicting views on the lawfulness of such IO); Doswald-Beck, *supra* note 58, at 171 (arguing that attacking an adversary while giving the impression of coming from the adversary's own side would be illegal).

unanticipated uses of IO or even move states to respond to IO with physical force. Alternatively, states may avoid IO's uncertainty, and decline to employ it entirely. For example, during the 1999 Kosovo conflict, widely circulated reports described how plans to conduct an IO depleting Serbian leader Slobodan Milosevic's personal financial holdings were never executed.[97] Of course, when militaries avoid IO that usually means they rely instead on traditional weaponry, which may actually cost more lives and damage than a more novel IO method.

The lack of clarity also has individual effects since certain violations of the law of war (e.g., civilian distinction) constitute war crimes. We live in an era of increasing individual legal responsibility at national and international levels. Today, war crimes charges can arise in Belgian or German courts, not to mention the International Criminal Court.[98] Although jurisdictional hurdles may make prosecutions of U.S. forces unlikely, that will not stop investigations or even indictments if these institutions interpret some IO as violating the law of war.[99] Moreover, the "CNN factor" makes allegations of war crimes a matter of public discourse, rapidly dispersed through media outlets and information networks worldwide. In this environment, it is not surprising that military commanders may shy away from IO, especially if they do not know which conduct will lead to war crimes allegations. Looking at Kosovo again, the United States apparently refrained from planned CNA against Serbian computer networks for purposes of disrupting military operations and basic civil services in part due to concerns that some such CNA would be a war crime.[100]

B. Insufficiency & Complexity

Even if greater certainty existed on how to apply the law of war to IO, that body of law remains insufficient to address all the circumstances in

---

[97] Dunlap, *supra* note 65, at 363.

[98] *See, e.g.*, Rome Statute of the International Criminal Court, art. 5, July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute]; Diane F. Orentlicher, *Whose Justice? Reconciling Universal Jurisdiction with Democratic Principles,* 92 GEO. L.J. 1057, 1060–61 (2004) (surveying international criminal complaints raised in national courts); Mohamed M. El Zeidy, *Universal Jurisdiction* In Absentia*: Is It a Legal Valid Option for Repressing Heinous Crimes?,* 37 INT'L LAW. 835, 842–49 (2003) (discussing universal jurisdiction provisions in the domestic laws of Austria, Belgium, Germany and Spain).

[99] The Rome Statute limits the ICC's jurisdiction to cases where the defendant is either a national of a state party or the conduct occurs in the territory, aircraft, or vessel of a state party (non-state parties may also accept the Court's jurisdiction under the same conditions). Rome Statute, *supra* note 98, art. 12(2). Status of Forces Agreements (SOFAs) may also limit a host nation's ability to conduct criminal prosecution of visiting U.S. forces. *See, e.g.*, Agreement Between the Parties to the North Atlantic Treaty Regarding the Status of Their Forces, art. VII, June 19, 1951, 4 U.S.T. 1792 [hereinafter NATO SOFA] (delineating jurisdiction over sending state forces).

[100] Silver, *supra* note 65, at 74.

which IO may occur. The law of war provides little guidance for regulating asymmetric uses of IO between state and non-state actors. And where states employ IO in ways unregulated by the law of war or by the prohibition on the use of force, a dizzying array of legal regulations threatens to overwhelm a state's ability to use, or even defend against, IO.

The law of war is state-centric, primarily regulating how states can employ force against other states. Thus, analogizing the law of war to IO will, at best, establish a set of rules for inter-state IO that forms a *lex specialis* in covered conflicts. Most scholars and officials appear comfortable with that outcome. Current efforts to apply international law to IO by analogy have focused almost exclusively on its application to international armed conflicts between two or more nation-states.[101] Although such conflicts retain undoubted importance, it is a mistake to force all discussion of IO into this interstate conflict paradigm. Today, the center of gravity is shifting in a different direction. Future conflicts will more likely pit states against non-state actors, such as al-Qaeda, than other nation-states.[102] Current conditions in Iraq and Afghanistan demonstrate, moreover, that even conflicts between states will frequently devolve into conflicts with non-state actors, whether as insurgents or terrorists. When combined with the novelty and variety of IO, such shifts

[101] The analyses tend to focus alternatively on the *jus ad bellum* or the *jus in bello*. *See, e.g.*, SHARP, *supra* note 73 (examining *jus ad bellum* in cyberspace); Anderson & Dooley, *supra* note 65, at 268 (focusing on acts by or on behalf of states); Brown, *supra* note 35, at 180–81 (assessing *jus in bello* and information warfare); Dörmann, *supra* note 78, at 1 (focusing "essentially on international armed conflicts"); Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework,* 12 EUR.J.INT'L L. 825, 828 (2001) (assessing information warfare under use of force rules); O'Donnell & Kraska, *supra* note 94, at 139 (examining international humanitarian law); Schmitt, *supra* note 29, at 888 (exploring *jus ad bellum* and CNA); Schmitt II, *supra* note 33, at 367 (addressing use of CNA "during *international* armed conflict"); Mark R. Shulman, Note, *Discrimination in the Laws of Information Warfare,* 37 COLUM. J. TRANSNAT'L L. 939, 942 (1999) (concentrating on the *jus in bello*); Jensen II, *supra* note 65, at 1150–51 (*jus in bello*). A smaller body of work has considered IO in a broader context. *See, e.g.*, *DOD GC Memo*, *supra* note 63 (comprehensive review of legal issues raised by CNA); Condron, *supra* note 12, at 421 (favoring an expansion of *jus ad bellum* to allow active defenses against all attacks on critical infrastructure without requiring attribution or characterization of the attack); Barkham, *supra* note 12, at 57 (examining *jus ad bellum* as well as impact of non-state actors on existing system); Haslam, *supra* note 70, § 4.3, at 165 (assessing information warfare in terms of the law of intervention, prohibitions on the use of force, and the law of war).

[102] *See, e.g.*, Brooks, *supra* note 23, at 710 (describing the "rise of global terrorism" as the "newest and most serious challenge to the old law of armed conflict framework"); BOOT, *supra* note 46, at 471–72 (discussing need for militaries to address dangers of terrorist and guerrillas alongside conventional threats). Thus, my argument holds regardless of whether one accepts the enlarged definition of international armed conflicts under Additional Protocol I.

reveal the insufficiency of existing analyses. IO must be considered as more than something states in conflict do to each other.[103]

The law of war, however, has only a limited reach beyond international armed conflicts, and even where it applies, it does so with relatively few requirements. Thus, the laws governing an "armed conflict not of an international character occurring in the territory" of a party could apply to IO.[104] Debate continues, however, over whether all armed conflicts qualify as international or non-international, or if some gap exists free from regulation (e.g., an international conflict with a non-state actor rather than a state).[105] Even if the non-international armed conflict rules apply, they give much less guidance on when and how states can use IO than rules, uncertain as they are, involving IO in international armed conflicts. For example, there is no "non-international" counterpart to the use-of-force prohibition that might restrain when states can use force in such conflicts. Although Common Article 3 of the Geneva Conventions does apply, it has little relevance to IO, given its focus on humane treatment for individuals not actively participating in the conflict. Additional Protocol II—which governs classic civil wars—has a few rules relevant to IO by analogy, including a prohibition on making civilians the object of attack and protecting certain installations.[106] But Additional Protocol II requires no protection for civilian objects, nor does it prohibit perfidy. The ICRC has recently suggested—not without opposition—that customary international law fills in many of these gaps, importing rules similar to those found in Additional Protocol I such as civilian distinction and rules on deception.[107] Of course, even if true, that simply replicates in the non-international context the same translation problems posed for regulating IO in international armed conflicts.

---

[103] One area where the existing law of war does contemplate regulating individual acts against a state is the rules governing state treatment of spies and saboteurs, but it links the authorized treatment of such persons to their location within occupied territory—a concept that may not have as much relevance in the IO context given the ability of non-state actors to perform IO from virtually anywhere in the world. *See, e.g.,* GC IV, *supra* note 53, art. 5 (allowing states to forfeit communication rights for spies or saboteurs detained in occupied territory where absolute military security so requires).

[104] *See* GC I, *supra* note 53, art. 3 (common to all four Geneva Conventions).

[105] For the United States at least, the U.S. Supreme Court recently answered that question in the negative. *See* Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2795 (2006). For a discussion of the pre- and post-*Hamdan* position of the U.S. Executive Branch, *see* Posting of John Bellinger to Opinio Juris, http://www.opiniojuris.org/posts/1169777773.shtml (Jan. 25, 2007).

[106] AP II, *supra* note 61, arts. 11–13.

[107] Jean-Marie Henckaerts, *Study on Customary International Humanitarian Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict*, 87 INT'L REV. RED CROSS 175, 189 (2005), *available at* http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/review-857-p175/$File/irrc_857_Henckaerts.pdf. For U.S. views critical of the ICRC study, *see* Posting of John Bellinger to Opinio Juris, http://www.opiniojuris.org/posts/1169328256.shtml (Jan. 20. 2007).

The most important questions occur when the law of war does not apply to IO—even by analogy—because the IO does not constitute an armed attack, since that will be where states and non-state actors will most likely collide.[108] Although militaries have devoted extensive time to developing IO capabilities and doctrines, non-state actors can perform IO as well. IO technology remains widely accessible, much less expensive than traditional kinetic weaponry, relatively easy to use, and capable of deployment from virtually anywhere in the world.[109] As such, IO is particularly attractive to non-state actors—including transnational criminal and terrorist elements—looking to target public or private interests.[110]

Once IO leaves the law of war paradigm, however, state options to conduct or defend against IO become much more limited. Absent state sponsorship, where IO (or indeed any form of attack) has non-state actor origins, those origins may preclude it from qualifying as an armed attack and, thus, deprive states of a right to respond in self-defense.[111] Although not without controversy, the International Court of Justice has opined that self-defense is not an option when dealing with non-state actors; states are expected to deal with them through domestic law enforcement, not military coercion.[112] Even if a victim state traces CNA to a non-state actor operating in another state's territory—no easy task given the ability to mask CNA's origins and route it through multiple states—it cannot respond directly. To do so would implicate one of the core principles of

[108] I argue IO involving state and non-state actors will most often fail to qualify as an armed attack for both empirical and legal reasons. Empirically, IO's effects are more likely to involve temporary disruptions or deceptions than the death or destruction that characterizes an armed attack. *See supra* notes 36–40 and accompanying text. Legally, there is the argument that non-state actors cannot commit an armed attack so that all non-state-actor IO would lie beyond the law of war's reach. *See infra* notes 112–17 and accompanying text.

[109] Condron, *supra* note 12, at 404 (citing low cost, wide availability and ability to accomplish military objectives using computers).

[110] *But see* Dunlap, *supra* note 65, at 359 (arguing that the absence of any catastrophic events caused by IO demonstrates that IO may be more difficult to accomplish than theorists realize, but conceding that IO still poses a threat in certain contexts, such as IO's capacity to steal identities).

[111] *See supra* note 67, and accompanying text.

[112] *See, e.g.*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, July 9, 2004, 43 I.L.M. 1009, 1050 (ICJ 2004); *accord* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, ¶¶ 146–47 (Dec. 19); Condron, *supra* note 12, at 414–15; Silver, *supra* note 65, at 93; Barkham, *supra* note 12, at 72. The U.S. State Department Legal Adviser, however, has taken an opposing view. Posting of John Bellinger to Opinio Juris, http://www.opiniojuris.org/posts/1168811565.shtml#2795 (Jan. 15, 2007); *see also Armed Attack*, *supra* note 22, at 45–50 (despite lack of "widespread acceptance by the global community" that terrorist attacks can constitute armed attacks justifying a self-defense response, arguing that the September 11, 2001 incidents qualify as such, and tracing the origins of the self-defense doctrine to attacks by non-governmental entities, e.g., U.S. nationals' support for a rebellion in Canada that led to the *Caroline* incident).

the international legal order: the principle of non-intervention, which provides a state with the right to be sovereign within its own territory, free from external interference.[113] A state will view another state's exercise of military or law-enforcement powers within its territory as a violation of that sovereignty.[114] What should an injured state do? International law contemplates that the injured state would notify the state from whose territory it believes the IO originated and request that state put a stop to it.[115] The requested state is expected to comply with such requests, which explains the latest tension between Estonia and Russia over Estonia's investigation of the attacks against it.[116] Only if the requested state is unable or unwilling to stop the IO can the aggrieved state take counter-measures (or perhaps exercise a right of self-defense against the requested state like the United States did against Taliban-ruled Afghanistan).[117]

Ironically, even as the current legal framework for IO exhibits insufficiencies in its application to the new realities of asymmetric conflict, it proves exceedingly complex in other respects. Such complexity is most visible in terms of the rules for states that want to deploy IO offensively without triggering the prohibition on the use of force (assuming they can overcome the translation hurdles to make that call). For such IO, states have not one, not two, but more than a half dozen different legal regimes to assess in deciding whether and how to proceed. First, as discussed above, a state considering offensive IO must assess the principle of non-intervention and whether its IO will improperly affect the territory of another state. States are likely to view injury or physical damage as interfering with their sovereign rights, but not all effects will so qualify. Consider espionage—the covert collection of information about other states, often in the other state's territory.

[113] *See, e.g.*, 3 E. DE VATTEL, THE LAWS OF NATIONS OR THE PRINCIPLES OF NATURAL LAW 19 (Charles G. Fenwick trans., James B. Scott ed., 1758) (describing consensus against "intermeddl[ing] in the domestic affairs of another Nation"); Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 106 (June 27) ("The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; . . . it is part and parcel of customary international law.").

[114] *See* John F. Murphy, *Computer Network Attacks by Terrorists: Some Legal Dimensions*, 76 INT'L L. STUD. 321, 338, 342 (2002) [hereinafter *Computer Network Attacks by Terrorists*] ("Unconsented to transborder searches of electronic evidence may be viewed by the country where the search occurs as a violation of its sovereignty or even of its criminal law, subjecting the individual investigator to possible criminal liability.").

[115] *DOD GC Memo*, *supra* note 63, at 487–88; Dinstein, *supra* note 65, at 103. According to the *Corfu Channel* decision, every state is under an obligation "not to allow knowingly its territory to be used for acts contrary to the rights of other States." Corfu Channel (U.K. v. Alb.) 1949 I.C.J. 4, 22 (Apr. 9).

[116] *See supra* note 19 and accompanying text.

[117] *See* Responsibility of States for Internationally Wrongful Acts, art. 49, G.A. Res. 56/83, Annex, U.N. Doc. A/56/10/Annex (Dec. 12, 2001); *DOD GC Memo*, *supra* note 63, at 488.

Although states generally treat espionage as violating their domestic law, it does not violate any explicit provisions of international law and states widely engage in it.[118] As a result, the application of the non-intervention principle may depend on the method of IO used, i.e., whether it merely is collecting data as opposed to altering, usurping or destroying it.

Second, states need to adjust their IO to satisfy their obligations under various specialized regimes of international law. For example, because information infrastructures frequently use outer space to relay communications or collect data, space law may affect IO. Under Article IV of the Outer Space Treaty, states have agreed to use the moon, other celestial bodies, and by extension, space itself "exclusively for peaceful purposes."[119] Although this does not automatically preclude lawful military activity in space, determining the contours of "peaceful purposes" has long been a subject of debate that IO will only make worse. Moreover, Article IX of the Outer Space Treaty imposes a notice and consultation requirement before a state engages in any IO that it believes "would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space."[120] A similar obligation exists under the Constitution of the International Telecommunications Union (ITU). Article 45(1) requires that all telecommunications stations operate so as not to cause "harmful interference" to other radio services or communications carried on in other states.[121] In both situations, states need to consider forgoing IO effects that might constitute harmful interference (e.g., jamming radio broadcasts).[122] If for some reason IO involves data streams transiting (or otherwise relating to) the sea or civilian airspace, additional legal regimes constrain IO. Article 19 of the 1982 United Nations Convention on the Law of the Sea, for example, prohibits states from prejudicial acts when exercising the right of innocent passage through another state's territorial sea, including activities that could be IO such as information

[118] *DOD GC Memo*, *supra* note 63, at 516; Tubbs, Luzwick & Sharp, *supra* note 65, at 16; Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law,* 27 MICH. J. INT'L L. 1071 (2006).

[119] *See, e.g.,* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, art. IV, *done* Jan. 27, 1967, 18 U.S.T. 2410 [hereinafter The Outer Space Treaty].

[120] *Id.* art. IX; Anderson & Dooley, *supra* note 65, at 281–82.

[121] Constitution of the International Telecommunication Union, art. 45(1) (1999) [hereinafter ITU], *available at* http://www.itu.int/aboutitu/Basic_Text_ITU-e.pdf. Harmful interference is defined as "[i]nterference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the [ITU] Radio Regulations." *Id.*, Annex, 1003.

[122] In the ITU, however, the prohibition does not apply to military radio stations, which may reopen the door to otherwise prohibited acts. *Id.* art. 48(1) ("Member States retain their entire freedom with regard to military radio installations.").

collection, interference with communications systems, and propaganda.[123]

Other treaty regimes, however, may have no real effect on a state's deployment of IO. Despite the current dominance of the criminal law paradigm for responding to malicious uses of computer networks, that paradigm avoids regulating the deployment of IO by states. The Cybercrime Convention perpetuates deference to state sovereignty by requiring parties to criminalize various forms of computer misuse by non-state actors. Its rules, however, do not apply to government activities, whether for law enforcement or national security purposes.[124] Similarly, despite terrorists' ability to use and defend against IO, none of the terrorism conventions speaks to IO, and these treaties have little to say about terrorist uses of the Internet, the media, or other communication networks.[125]

Finally, states contemplating IO must assess how other states' domestic laws come into play.[126] States whose territory is the target of an IO may apply their criminal law based on effects within their territory. States through whose territory IO data streams transit en route to their destination may do the same. Moreover, if a military conducts IO from an overseas base, the law of the host nation can regulate that conduct and form a basis for prosecuting individuals engaged in the IO. Although Status of Forces Agreements (SOFAs) may protect these individuals sent overseas if acting in their official capacity, that protection often only applies where both the sending and receiving state recognize the offense.

---

[123] *See, e.g.*, United Nations Convention on the Law of the Sea, arts. 19, 109, *concluded* Dec. 10, 1982, 1833 U.N.T.S. 396 [hereinafter UNCLOS]. The United States regards UNCLOS as generally codifying customary international law.

[124] *See* Cybercrime Convention, *supra* note 26. Article 2, for example, requires states to adopt "legislative and other measures" to establish as criminal offenses under their domestic law intentional "access to the whole or any part of a computer system without right." *Id.* The accompanying Explanatory Report clarifies that the "without right" caveat "leaves unaffected conduct undertaken pursuant to lawful government authority" including acts to "protect national security or investigate criminal offences." Council of Europe, Convention on Cybercrime, Explanatory Report, C.E.T.S. No. 185, ¶ 38 (Nov 8, 2001), http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. That reference suggests the negotiators were well aware of states' developing IO doctrines and sought to draft around them in this Convention.

[125] In several instances, however, the acts criminalized by these treaties might include using information networks as part of the commission of the criminal offense, although none of them regulate or criminalize the use of such information networks specifically. *See, e.g.*, International Convention for the Suppression of the Financing of Terrorism, art. 2, *adopted* Dec. 9, 1999, 39 I.L.M. 270, 2178 U.N.T.S. 228 (making it an offense to "directly or indirectly" provide or collect funds by any means with the intent or knowledge that they relate to the commission of terrorist acts); Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, art. 1, Sept. 23, 1971, 24 U.S.T. 565, 974 U.N.T.S. 177 (making it an offense to destroy or damage air navigation facilities or interfere with their operation or to communicate false information that endangers the safety of an aircraft in flight).

[126] *DOD GC Memo*, *supra* note 63, at 513–14.

If the IO is only a crime under the receiving state's laws, it retains exclusive jurisdiction.[127] Accordingly, depending on its content—which will vary enormously—foreign law may have significant implications for IO.

Combined, these two problems—the insufficiency of the law of war and the multiple, overlapping legal regimes outside the law of war paradigm—produce a system that is extraordinarily hard for states and their militaries to navigate. If, as David Kaye suggests, complexity in the law of war itself is already a problem for those who use force, IO only compounds that problem given the array of additional legal rules to consider, interpret, and apply.[128] Government and military lawyers will have great difficulty in processing all these issues simultaneously, particularly in situations where they may be asked to react immediately. Do we necessarily want the disincentive to use IO that such confusion creates where the alternatives may be traditional uses of force or doing nothing? We have a system, which in its uncertainty, insufficiency, and complexity does just that. Wouldn't states prefer, instead, a framework that does not simply restrict IO, but also facilitates IO in cases where it might be easier to use, cause less harm, or prove more effective than traditional alternatives in combating new threats like global terror? In other words, perhaps the conventional wisdom on the viability of IO law by analogy is simply wrong.

V. ILIO'S BENEFITS

Devising a system of international law for information operations (ILIO) could rectify many of the deficiencies of the current legal system and provide states with additional functional benefits that do not currently exist. First, ILIO can remedy uncertainty. Drafting new rules provides an opportunity to rectify translation problems that plague IO under the law of war. It could give states and their militaries a clear sense of the rules of engagement in the information age. For example, ILIO would allow states not simply to choose among available interpretations of the prohibition on the use of force, but to craft a standard tailored to IO without the additional over- or under-inclusion problems that currently exist. Similarly, states could set the bar for when IO triggers the civilian distinction requirement and address whether any or all information networks constitute legitimate military objectives. Of course,

[127] *See, e.g.*, NATO SOFA, *supra* note 99, art. VII(2)(b) ("The authorities of the receiving State shall have the right to exercise exclusive jurisdiction over members of a force or civilian component and their dependents with respect to offences, including offences relating to the security of that State, punishable by its law but not by the law of the sending State." Security offenses are defined to include "sabotage, espionage or violation of any law relating to official secrets of that State, or secrets relating to the national defence of that State.").

[128] *See generally* David Kaye, *Complexity in the Law of War*, *in* PROGRESS IN INTERNATIONAL ORGANIZATION (2007).

ILIO does not have to supplant the existing system entirely; it can easily preserve basic principles that continue to make sense—such as the rule requiring military necessity in using force—while adjusting others (e.g., perfidy) to fit the context in which IO occurs.[129]

Why not wait—as the ICRC suggests[130]—and rely on what states actually do in lieu of negotiating an ILIO? Assuming state practice coalesced into customary international law, this could function as an alternative remedy for the current uncertainty problem. But adopting a state practice approach will not necessarily overcome the law's current insufficiency or its complexity. For example, a customary ILIO is unlikely to simplify the law into a single, codified set of rules in the same way a more affirmative negotiation of ILIO among states would. Adopting a customary international law approach also presents new problems that ILIO avoids. For starters, it can take years or decades for state practice to coalesce into customary international law. In the interim, states will remain confused and wary of IO, which may not be a desirable result in all circumstances. Second, attribution issues may make it difficult to ever discern state practice in IO. IO's strength often lies in its anonymity and secrecy—victims of IO may not know that they have been subjected to it, let alone who is responsible (although constantly changing technology ensures that this will not always be the case).[131] Thus, we may not know what a state believes the law to be, until caught and forced to justify a particular IO (assuming the victim state wants to publicize the IO, rather than respond in kind). Ironically, this means states with weaker IO skills may actually take the lead in providing evidence of a state practice on IO. In contrast, by discussing ILIO prospectively, states with more sophisticated IO doctrines and capabilities would have an opportunity to set the agenda for a regulatory framework free from operational security constraints. Through an ILIO-making exercise, participants would gain a sense of ownership over the legal framework that might be absent if customary international law were the only basis for rule-making. This could achieve greater certainty in the conduct of future IO, even if still done in secret.

The need for greater certainty is particularly acute for the United States. Although it clearly has a comparative advantage in terms of IO technology, the United States is simultaneously the most vulnerable to IO given its society's constantly increasing dependence on information and

[129] For some, however, the notion of ILIO might operate in tension with the Internet's purported "borderless" nature, one not controlled by governments but subject to private innovation and few controls. *See* Wedgwood, *supra* note 94, at 227; Condron, *supra* note 12, at 409. Although that may have constituted the original vision, states have increasingly demonstrated that the Internet does have borders and that states can control them. *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? (2006).

[130] Dörmann, *supra* note 78, at 3.

[131] Barkham, *supra* note 12, at 64; Silver, *supra* note 65, at 78–79.

information networks.[132] In such circumstances, U.S. interests should favor ILIO. It presents an opportunity to develop rules that could cement U.S. comparative advantage while mitigating existing vulnerabilities. Of course, other states with less developed IO capabilities are aware of this situation and might be reluctant to endorse ILIO because of it.

On the other hand, ILIO could include functional benefits luring even reluctant states to the bargaining table. Currently, the rules applicable to IO by analogy are largely restrictive; limiting what states can do in the interest of maintaining international peace and security, protecting civilian populations, and prohibiting morally reprehensible conduct. But those interests may not always be served only by restricting IO. If we live in a world where the threat to states is no longer primarily from other states but from non-state actors, do we serve international peace and security by imposing so many restrictions on how states use IO against non-state actors? What happens when al-Qaeda launches its own IO against one or more states?[133] States might wish to have fewer restrictions or actual authority to respond to that IO in self-defense or in kind. Similarly, do we want states to forgo IO's more effective and humane methods in favor of continued uses of physical force? Perhaps states should allow IO a wider, albeit virtual, impact on civilian populations if the result is less physical harm overall, or even on an individual basis, than traditional warfare.

Such possibilities suggest that we conceive of the ILIO project not simply as refining restrictions on IO, but actually *enabling* it in circumstances that advance the common interests of states. For example, rather than seeing ILIO as essentially a question of restricting what states do to one another, ILIO could establish rules enabling states to better meet the challenges posed by non-state actors, particularly those bent on global terror. In the language of economists, ILIO may reduce the transaction costs that states face in combating transnational terrorism. The current system—which might prohibit a state from responding to an al-Qaeda IO attack from Pakistan directly or immediately, requiring it instead to ask Pakistan for assistance—is not terribly efficient and may have high costs for the victim state's safety and security. In its place, ILIO offers an opportunity for states to acknowledge their collective interest in combating non-state terrorist actors as a threat to the state system itself, and to devise cooperative mechanisms that increase the efficiency of such efforts. This might involve, for example, states such as Pakistan consenting to suspend the non-intervention principle in certain pre-agreed circumstances and allowing injured states to respond immediately and directly to IO generated from their territory (i.e., to conduct an active defense to CNA). Or, perhaps states could establish a program where a state sends information officers to other states who can approve

[132] *See* Schmitt, *supra* note 29, at 936.

[133] *See* Condron, *supra* note 12, at 405 (discussing reports of an al-Qaeda interest in acquiring IO capabilities).

IO methods that target or transit the sending state's territory. There is already some precedent for this in the maritime context, through the practice of "shiprider" agreements, in which a foreign state agrees that one of its officials may serve aboard a U.S. ship and authorize it to conduct law-enforcement activities against ships of that foreign state and even within the foreign state's territorial seas.[134]

At the same time, let me be clear—developing new rules does not mean sacrificing the bedrock rationales for the existing legal system, especially those applicable in international armed conflicts, such as reciprocity or prohibiting morally reprehensible conduct. To the extent the current law of war relies extensively on the principle of reciprocity, ILIO can operate as a bargain among the consenting states in much the same way. ILIO's translation of the use of force prohibition would undoubtedly retain the principle's inherent reciprocity—i.e., each state agrees to refrain from force, however defined, so long as the other side does so as well. Similarly, to the extent the law of war also has a universal or moral basis (i.e., states do not engage in certain acts even if done by the adversary because they deem such acts morally reprehensible), nothing precludes ILIO from accommodating that basis as well (e.g., IO-tailored rules on perfidy). In other words, in rejecting the current law-by-analogy approach, ILIO does not need to dispense with analogies to existing principles (or even specific rules) entirely. The point of ILIO is to afford a considered process in which states devise new rules in ways that afford more certainty to the use of IO than the current framework and facilitate its usage in appropriate situations (e.g., where it will impose fewer costs, less harm, or achieve objectives more efficiently than blunt applications of physical force).

Of course, ILIO will not come without costs or risks of its own. Interested states will undoubtedly have to devote substantial resources to negotiating this new set of rules. Given the frequently secretive and surreptitious nature of ILIO, states may find such negotiations hampered by the lack of information on the full scope of states' IO capabilities and doctrines, not to mention the technical problems associated with attributing the sources of IO that may be necessary to have any corresponding rules on its use or responses to its use. Privacy interests and free speech concerns may also emerge to counterbalance state interests in more expansive uses of IO. As a result, there is a real possibility that states could fail in their efforts to devise an ILIO. Even if successful in devising some new normative framework, however, other

[134] *See, e.g.*, Agreement between the Government of the United States of America and the Government of Jamaica Concerning Cooperation in Suppressing Illicit Maritime Drug Trafficking, U.S.-Jam., May 6, 1997, K.A.V. 5155, 1998 WL 190434. Of course, such cooperative efforts would need to be calibrated to protect legitimate privacy interests, even as they facilitate the fight against terror. *See Computer Network Attacks by Terrorists*, *supra* note 114, at 344; *see also* Condron, *supra* note 12, at 418–19 (suggesting need to rebalance civil liberties and national security concerns in context of cyber attacks).

states may consciously decide to opt out or "free ride," weakening the viability of the new system. In addition, as with any regulation of technology, a set of rules that makes sense today could become obsolete or even defective tomorrow should either IO technology or its targets change.

The risks of an ILIO, however, do not dictate a return to the status quo. Issues of transaction costs, free riders, and technological change accompany virtually all efforts to update, revise, or expand international law. Moreover, many of the costs and risks can be mitigated by building safeguards into the regulatory regime that expresses the ILIO. For example, states could tie legal effect of an ILIO to a minimum level of participation by states or groups of states. Similarly, surmounting the changing technology problem may simply be a function of defining IO in ways that would accommodate and include technological innovation, much like what the Martens Clause does for the law of war currently.[135]

Finally, ILIO offers an opportunity for the law of war more generally. It is no secret that the law of war has proven largely inadequate in addressing non-international armed conflicts. For the most part, states see such conflicts as implicating their sovereignty, or even their very survival, at levels not presented in conflicts with other states. Similarly, when the conflict only involves one state actor versus a non-state actor, the reciprocity rationale for the law of war is largely absent. As a result, states have been reluctant to agree to detailed rules for such conflicts. For ILIO, however, many of the sovereignty concerns are—if not non-existent—at least diminished. IO will frequently lack any direct territorial impact with its effects limited to the virtual world or other information networks. IO's impacts can be temporary and more easily remedied than the casualties and destruction so often witnessed in civil wars and other internal conflicts. Moreover, the non-state actor threat often transcends the territorial ambitions that dominated the post-colonial era. To the extent that actors like al-Qaeda constitute a threat, it is not simply to certain nation-states and their territorial integrity, but to the very concept of a system of secular, equally sovereign states. As such, unlike past non-international conflicts, there is a reciprocity concern here—not a concern of reciprocating restrictions, but reciprocating cooperation to forestall a common threat. ILIO offers an opportunity to do this. It provides states a chance to devise rules not only for their inter-state relations, but also in areas that have so far proven difficult to regulate—international law requirements for non-international armed conflicts and cases short of actual armed conflict.

VI. CONCLUSION

Conventional wisdom's favored law-by-analogy approach has clear flaws. Its translation to IO is rife with uncertainty and complexity, which

[135] *See supra* note 53 and accompanying text.

will result in less IO or greater conflict among states, courts, and international institutions about what international law requires of IO. At the same time, a law of war or use of force effort to regulate IO is clearly insufficient where the fight with al-Qaeda, the Taliban, and other insurgents typify future conflicts far more than old inter-state conflicts. The need for ILIO becomes even more apparent as the uncertainty of IO under the law of war is magnified and compounded in trying to discern the array of rules that govern IO outside of an inter-state armed conflict. Such deficiencies in the status quo beg for a new framework. A new framework could not only remedy the existing system's deficiencies, but offer additional advantages of its own. States may adopt cooperative mechanisms—common tools to address new threats—preserving their strengths in IO technology while shoring up against their individual vulnerabilities to IO.

Obviously, the structure and content of an ILIO framework can (and should) be subject to great debate. The few suggestions so far have idealized a multilateral treaty akin to the Geneva Conventions that could contain precise and detailed rules on IO.[136] But that may be an overly ambitious, if not misguided, approach to establishing an ILIO, given the difficulty of obtaining sufficient state participation and rules that can adapt to future technological changes. In reality, states seeking to devise an ILIO face a larger (and more complex) set of regime choices, involving questions of (i) who should make the ILIO; (ii) what form the rules should take; (iii) the role of institutions in overseeing ILIO's implementation and enforcement; not to mention (iv) the actual content of the rules themselves and their capacity to change over time.[137]

Certainly, we could envision all states realizing the normative attraction of an ILIO and crafting a large treaty to accommodate it.[138] But

[136] *See, e.g.*, Brown, *supra* note 35, at 215–21 (proposing a treaty to regulate the use of information systems in armed conflict); Barkham, *supra* note 12, at 112–13 (suggesting a treaty regime to regulate information warfare and discussing advantages and obstacles to such a result).

[137] Similar questions arise in other areas where technological developments suggest a need for legal regulation. *See, e.g.*, Kenneth Abbott et al., International Regulatory Regimes for Nanotechnology, (draft manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=907353.

[138] For example, many states quickly recognized the threat posed by blinding laser weapons, negotiating and concluding a convention on the subject in 1995 that now has 86 state parties. *See* Protocol on Blinding Laser Weapons: Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Oct. 13, 1995, 2024 U.N.T.S. 163. In 1997, more than 150 states negotiated and concluded the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction. The United States, however, has not joined this treaty because of substantive concerns, which creates obvious problems in terms of universal adherence to its content. *See* Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, Sept. 18, 1997, 36 I.L.M. 1507; *see also* Amy F. Woolf, Steve Bowman & Sharon Squassoni, Arms Control

the path to creating international law need not always occupy the global stage. Perhaps the starting point for ILIO, like the law of war itself, might best lie in one or more individual nation-states producing a set of self-governing rules for their own IO and responses to IO directed against them; i.e., a modern Lieber Code for IO.[139] Or, a group of interested states might decide to articulate an ILIO among themselves, as the Council of Europe did for Cybercrime; certainly that is one outcome that might emerge from further NATO consideration of the Estonia attacks.[140]

Beyond the question of who makes ILIO, separate structural choices will be required as to the appropriate form ILIO should take. First and foremost, states need to decide whether to begin with international law at all, or if they prefer, to establish a set of non-legally binding norms with the expectation that international legal rules will emerge from them in time.[141] For example, ILIO could begin with efforts by states—alone or together with non-state actors such as the Internet Corporation for Assigned Names and Numbers (ICANN)[142], internet service providers, or

and Nonproliferation: A Catalog of Treaties and Agreements, (Cong. Research Serv., CRS Report for Congress Order Code RL33865, January 29, 2007), *available at*, http://fpc.state.gov/documents/organization/81995.pdf.

[139] *See generally* RICHARD SHELLY HARTIGAN, LIEBER'S CODE AND THE LAW OF WAR 45–72 (1983) (reprinting General Orders No. 100). National approaches would have the advantage of allowing experimentation among states as to the best balance of limiting and authorizing IO, while also accommodating the real privacy concerns involved in any regulation of information networks. On the other hand, if individual approaches differ too greatly, the problems of uncertainty and complexity in the existing framework would remain.

[140] Bilateral treaties form another regulatory regime model in between national and regional formats. It seems unlikely that two states would only want to regulate IO *inter se*, but perhaps that situation might occur where the two states are responding to actual deployments of IO between them, as might be the case if Estonia and Russia ever decided to erect legal barriers to a repeat of the recent attacks.

[141] The practice of states concluding non-legally binding instruments is now "employed in almost every field of international relations." Anthony Aust, *The Theory and Practice of Informal International Instruments*, 35 INT'L & COMP. L.Q. 787, 788 (1986). States may thus choose to establish norms that have political or moral, as opposed to legal, force, either with the expectation that such a normative framework will prove sufficient or as a stepping stone to later legal regulation. *See, e.g.*, Maurice Copithorne, *National Treaty Law and Practice: Canada*, *in* NATIONAL TREATY LAW AND PRACTICE 2–3 (Duncan B. Hollis et al. eds., 2005) (comparing treaties with "international statements of intent or best efforts" which "while not binding in international law, do carry significant moral or political weight"); *see also* Dinah Shelton, *Introduction: Law, Non-Law and the Problem of "Soft Law*," *in* COMMITMENT AND COMPLIANCE 1, 10 (Dinah Shelton ed., 2000); W. Michael Reisman, *A Hard Look at Soft Law*, 82 AM. SOC'Y INT'L L. 371, 376 (1988); *see generally* Michael Bothe, *Legal and Non-Legal Norms—A Meaningful Distinction in International Relations*, 11 NETH. Y.B. INT'L L. 65 (1980); Oscar Schachter, *The Twilight Existence of Nonbinding International Agreements*, 71 AM J. INT'L L. 296 (1977).

[142] ICANN is a private non-profit organization that has responsibility for assigning Internet addresses and establishing Internet domains, with operations around the world, overseen by an internationally diverse board of directors. *See generally* ICANN, http://www.icann.org.

the telecommunication industry—to draft legally non-binding principles with the expectation that they might later become the subject of a treaty or other form of regulation.[143] Or, perhaps the starting point should be an experts' code of conduct like the San Remo Manual.[144]

Even assuming states agree on the treaty form as the best vehicle for creating an ILIO, however, they must decide on whether to begin with the rules themselves or with institutionalizing a process for crafting IO-specific rules in the future. Thus, rather than rely on the Geneva Conventions as the model for an ILIO, states could negotiate and conclude a "framework convention" that establishes common principles for their activities and leaves space for the negotiation of further protocols or amendments to provide the actual rules for conducting or defending against IO.[145] A related question will be the extent of centralization or institutionalization to impose alongside any substantive rules. States could establish institutional mechanisms or actually create an international organization to monitor and oversee when and how IO

[143] The prior informed consent procedure laid out in the Rotterdam Convention, for example, originally began as a voluntary system devised by states and the chemical industry to address the import and export of hazardous chemicals. Convention on the Prior Informed Consent Procedure for Certain Hazardous Chemicals and Pesticides in International Trade, Sept. 11, 1998, 38 I.L.M. 1. A similar cooperative effort by states and the diamond industry led to the Kimberley Process—a certification system designed to restrict trade in "blood diamonds" used to finance civil wars and other conflicts—which some states have now made legally binding as a matter of their domestic law. *See* Clean Diamond Trade Act, 19 U.S.C. §§ 3901–13 (2004); *see also* Brilliant Earth, Conflict Diamond Issues, The Kimberley Process, http://www.brilliantearth.com/dispcont.aspx?pageid=ABOUT_CONFLICT#Kimberly (overview of the Kimberley Process). Given the capacity of states and their militaries to employ or defend against IO, however, I do not think the starting point for ILIO lies in using industrial self-regulation increasingly seen in corporate codes of conduct. *See* David Kinley & Junko Tadaki, *From Talk to Walk: The Emergence of Human Rights Responsibilities for Corporations at International Law,* 44 VA. J. INT'L L. 931, 953–56 (2004) (discussing the corporate code of conduct phenomenon).

[144] INT'L INST. OF HUMANITARIAN LAW, SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Louise Doswald-Beck ed., 1995).

[145] This approach had great success in combating the threat of ozone depletion, but the verdict remains out on whether it can alleviate the threats posed by climate change and tobacco use. *See, e.g.*, Vienna Convention for the Protection of the Ozone Layer, Mar. 22, 1985, T.I.A.S. No. 11,097, 1513 U.N.T.S. 323 (treaty that led to the successful Montreal Protocol on Substances that Deplete the Ozone Layer); United Nations Framework Convention on Climate Change, May 9, 1992, 31 I.L.M. 849 (precursor to the Kyoto Protocol and any successor instrument); World Health Organization Framework Convention on Tobacco Control (2005) *available at* http://www.who.int/tobacco/framework/WHO_FCTC_english.pdf. For a more general discussion of framework conventions, see generally Daniel Bodansky, *Framework Convention on Tobacco Control: The Framework Convention/Protocol Approach,* WHO/NCD/TFI/99.1 (1999), *available at* http://whqlibdoc.who.int/hq/1999/WHO_NCD_TFI_99.1.pdf.

occurs.[146] If the political will exists, states could also follow the precedent in the arms control context of establishing verification procedures where other states or some designated non-state actor can examine state compliance with their ILIO obligations.

Finally, states will have to address ILIO's content, the extent to which ILIO should operate like those rules in the law of war that seek to control or prohibit technology, or like those rules that seek to control or prohibit certain conduct or effects. In doing so, states will also need to balance the law's proscriptive and permissive functions—i.e., the extent to which ILIO should restrict state behavior or require states to control IO that originates or transits their jurisdictions, versus the extent to which ILIO can enable states to use IO as an alternative to kinetic force, or in response to threats or attacks by non-state actors, especially those engaged in global terror. In the process, states will need to examine how to respond to anticipated (and unanticipated) technological developments—when and how ILIO obligations can change or adjust to avoid obsolescence, while respecting state sovereignty.[147]

Of course, all of this presumes that states and military thinkers appreciate the need to move beyond the law-by-analogy approach to IO. At present, states have not yet embraced this need. It remains to be seen, for example, if NATO member states will more fully engage the question of regulating IO in the aftermath of the Estonia attacks, or if they will continue along the current trajectory of employing criminal law tools and safeguards for CNA and other forms of IO. Thus, before states consider the content and structure of any ILIO, they must take the first step toward a new legal framework. To do so, states will have to recognize the deficiencies of the current system and the need, not to mention the advantages, that would flow from pursuing a new set of legal rules for information operations—an ILIO.

[146] For example, states might set up a "conference of the parties" that meets regularly to monitor ILIO and oversee its implementation and further development. *See, e.g.*, Robin R. Churchill & Geir Ulfstein, *Autonomous Institutional Arrangements in Multilateral Environmental Agreements: A Little-Noticed Phenomenon in International Law*, 94 AM. J. INT'L L. 623 (2000). Alternatively, states might rely on an existing organization like the ICRC to perform similar functions.

[147] *See, e.g.*, MALGOSIA FITZMAURICE & OLUFEMI ELIAS, CONTEMPORARY ISSUES IN THE LAW OF TREATIES 255 (2005) (discussing the possibility of states agreeing to tacit amendment of their treaty obligations that adjust certain treaty obligations for all states, in lieu of traditional procedures, where states individually consent to such changes or amendments).