OXFORD

CYBERWAR

Law and Ethics for Virtual Conflicts

EDITED BY
Jens David Ohlin, Kevin Govern, and Claire Finkelstein

Cyberwar

Law and Ethics for Virtual Conflicts

Edited by
JENS DAVID OHLIN
KEVIN GOVERN
CLAIRE FINKELSTEIN

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries

First Edition published in 2015

Impression: 2

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2014958038

ISBN 978-0-19-871749-2 (hbk)
ISBN 978-0-19-871750-8 (pbk)

Printed and bound by
CPI Group (UK) Ltd, Croydon, CR0 4YY

Cover image © Zap Art / GettyImages

Foreword

In 2013, the Group of Governmental Experts (GGE), a collection of cyber experts from fifteen states, concluded that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communications technology] environment."[1] Although drawing world-wide attention, the statement hardly represented a jurisprudential epiphany. Earlier the same year, the International Group of Experts (IGE) that produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare* agreed unanimously "both the *jus ad bellum* and the *jus in bello* apply to cyber operations."[2] Indeed, it is unfortunate that the GGE failed to explicitly pronounce on the applicability of the jus in bello (international humanitarian law (IHL)) to cyber operations occurring during an armed conflict.

Claims that cyberspace is a new domain to which international law is inapplicable (or inapplicable in part) persist but are steadily diminishing. The logic underlying the premise of international law's applicability to cyberspace is simply too compelling for such assertions to gain meaningful traction. For instance, in its *Nuclear Weapons Advisory Opinion*, the International Court of Justice confirmed that the UN Charter's Article 2(4) prohibition on the use of force and Article 51 acknowledgment of the "inherent" right of self-defense apply "regardless of the weapon used."[3] Today experts in the field universally accept this pronouncement as accurate. It is, therefore, difficult to sustain an argument that cyberweapons do not fall within its ambit. This is so despite occasional arguments that cyber operations do not involve the use of weapons. Such arguments, which tend to be advanced by those with little expertise in the jus ad bellum, were rejected by both the GGE and IGE.

Similarly, it is spurious to assert that IHL does not govern cyber operations during an armed conflict. Consider Article 36 of the 1977 Additional Protocol to the 1949 Geneva Conventions: "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."[4] This provision generally reflects customary law, and thus binds

[1] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para 19, UN Doc A/68/98, June 24, 2013, at <http://undocs.org/A/68/98>. The experts came from Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

[2] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013) 5.

[3] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226, para 39 (July 8).

[4] Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, art 36, June 8, 1977, 1125 UNTS 3.

all states irrespective of party status.[5] Since cyber operations involve "new weapon[s], means or method[s] of warfare," they, therefore, require review for compliance with the extant IHL. The Article unambiguously demonstrates that IHL was intended to continue to apply as the nature and instruments of warfare evolved. This is the position that has been taken by the International Committee of the Red Cross;[6] it is one that is, quite frankly, indisputable.

Although less studied, the applicability of international law to "below the threshold" cyber operations, that is, those that neither constitute a "use of force" nor an "armed conflict," would likewise appear certain. For instance, although it may sometimes be difficult to attribute cyber operations to a particular state, non-state actor, or individual as a matter of *fact*, there is no reason to exclude application of the *law* of state responsibility's attribution principles to them.[7] Similarly, on what basis would cyber operations conducted from land, sea, air, and space escape the reach, for instance, of the law of sovereignty, the law of the sea, air law, or space law? On the contrary—the risks associated with cyber operations to states, economies, societal functions, and individuals, make the argument for application of existing law especially compelling. As examples, the principle of due diligence can act to impede malicious cyber operations mounted from other states' territories by third parties,[8] while the plea of necessity affords a meaningful basis for responding to cyber operations against critical infrastructure in situations where even the originator of the cyber operation cannot be determined.[9]

Acknowledging that international law is applicable to cyber operations is only, however, the initial step in the process of articulating and implementing the normative architecture. Two more are necessary.

First, it is obviously essential to identify *how* that law applies. For instance, while it is clear that pursuant to the UN Charter and customary law, cyber uses of force are prohibited and forceful responses are only available once a cyber operation rises to the level of an armed attack, it remains unclear when a cyber operation qualifies as either a use of force or armed attack if it causes no physical damage or injury. The most oft-cited case is a massive cyber operation directed against a state economic infrastructure. Would the operation be unlawful as a prohibited use of force and would it qualify as an armed attack that allowed the target state to respond with its own forceful kinetic or cyber operations? Opinions vary.[10] Similarly, although the due diligence principle requires all states to take feasible measures to stop ongoing malicious cyber operations emanating from their territory that harm other states, what obligations does

[5] Tallinn Manual, Rule 48 and accompanying commentary. Although some states do not acknowledge the customary nature of the norm vis-à-vis methods of warfare, this minor deviation from the text of Article 36 has little bearing on the general applicability of IHL to cyber operations.

[6] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 31st International Conference of the Red Cross and Red Crescent, November 28–December 1, 2011, Doc 31IC/11/5.1.2, 36–7.

[7] UN International Law Commission, Report of the International Law Commission, Draft Articles of State Responsibility, Articles 4–11, U.N. GAOR, 53rd Session, Supp. No 10, U.N. Doc. A/56/10 (2001).

[8] Tallinn Manual, Rules 6–8 and accompanying commentary.

[9] Draft Articles of State Responsibility, Article 25.

[10] See discussion in commentary accompanying *Tallinn Manual* Rules 11 and 13.

that principle impose on a transit state in light of the difficulty of identifying malicious packets of data transiting their cyber infrastructure and the fact that a blocked transmission will often simply traverse a different route to the intended target?[11] And in the field of IHL, it is clear that attacks, including cyber attacks, against civilians and civilian infrastructure, are prohibited.[12] But when does a cyber operation qualify as an "attack" in the meaning of Article 49 of Additional Protocol I such that it is unlawful? Must it cause physical damage or injury? Or does interference with functionality qualify as damage? If so, what degree of interference?[13]

Second, the exercise of applying international law in the cyber context will reveal lacunae in the law that may need to be addressed directly through treaty action or that will inevitably become the subject of state practice that will in turn contribute to the crystallization of either responsive interpretations of existing law or new customary norms. To illustrate, IHL protects civilian objects against direct attack. The majority of the IGE concluded that data did not constitute a civilian object since they were intangible.[14] While this conclusion may be sound as a matter of legal interpretation, the consequences of the interpretation were seen as problematic even by some of the experts who took the position. Some data are plainly of great significance both to the orderly functioning of societies during an armed conflict and the general well-being of individuals. It would accordingly appear likely that over time a broader interpretation of the notion of objects in IHL will, and should, gain traction. The process of identifying such lacunae is essential if law is to adapt itself to the new realities of cyberspace.

Moreover, legal norms are but one facet of the normative universe. They merely articulate the outer limits of permissible cyber operations. Once these boundaries are defined, policy-makers craft ethical, political, and operational norms that further refine the permissible scope of cyber activities. The norms will find expression in domestic law or policy. They may also evolve into regional or global prescriptive norms. Thus, the work in these fields is no less important than that which is ongoing in the legal field. On the contrary, ethical, political, and operational norms may prove to have greater influence on restricting the conduct of cyber operations since legal norms sometimes allow states and other actors in cyberspace great leeway.

Unfortunately, non-legal cyber norms are too often conflated with legal ones. For example, ethicists speaking at the last two global CyCon conferences convened by the NATO Cooperative Cyber Defence Centre of Excellence, a leader in the field of cyber law and policy, repeatedly proffered ethical standards as binding international law. In doing so, they badly mangled the law. As the normative tapestry of cyber operations develops, it is essential that the various bodies of normative strictures be defined with precision. The process begins with international law boundaries for cyber operations and then those boundaries contract based on other concerns.

Cyberwar: Law and Ethics for Virtual Conflict measurably contributes to the process. It contains highly sophisticated legal analyses that not only apply extant international

[11] *Tallinn Manual* Rule 8 and accompanying commentary.
[12] Additional Protocol I, Article 52(1); *Tallinn Manual*, Rule 37.
[13] See discussion in commentary accompanying *Tallinn Manual*, Rule 30.
[14] *Tallinn Manual*, 127.

law in such areas as cyber deception and criminal law, but also tease loose such interpretive dilemmas as the classification of cyber armed conflict, the meaning of the term "attack," and the application of legal causality principles to cyber operations. The book also focuses on cyber activities that do not lend themselves well to the simple application by analogy of legal principles and rules developed in the non-cyber context. These topics include how the law responds to cyber operations mounted by individuals or non-state groups, including cyber terrorists, and whether traditional understandings of borders in international law are suited to application in cyberspace.

Recognizing that normative constraints are not exclusively juridical in nature, the book also explores the nature of cyberwar and its unique ethical status. Additionally, it usefully places cyber activities into a technical context, for norms, whether legal or not, must take cognizance of the distinctive technical environment to which they have to respond.

In this book, Jens Ohlin, Kevin Govern, and Claire Finkelstein have gatherd a distinguished and diverse group of contributors. They include accomplished scholars from different disciplines, as well as experienced practitioners. All have offered an especially perceptive perspective on their respective topics. Together their contributions take the discourse, which is too often counter-normative and usually stovepiped, to a new level. I congratulate the distinguished editors and contributors on their role in producing this fascinating and useful work.

Michael N Schmitt
Director, Stockton Center, United States Naval War College
Chair of International Law, Exeter University
Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence

Introduction

Cyber and the Changing Face of War

Claire Finkelstein and Kevin Govern

I. War and Technological Change

In 2012, journalist David Sanger reported that the United States, in conjunction with Israel, had unleashed a massive virus into the computer system of the Iranian nuclear reactor at Natanz, where the Iranians were engaged in enriching uranium for use in nuclear weaponry.[1] Operation "Olympic Games" was conceived as an alternative to a kinetic attack on Iran's nuclear facilities. It was the first major offensive use of America's cyberwar capacity, but it was seen as justified because of the importance of preempting Iran's development of nuclear weapons. The so-called "Stuxnet" virus successfully wreaked havoc with Iran's nuclear capabilities, damaging critical infrastructure and spreading massive confusion among Iranian scientists and engineers. The damage was comparable to a direct physical attack on Natanz, though perhaps even more debilitating, given the difficulties of attribution and the extremely covert nature of the attack.

Operation Olympic Games issued in a new era in national defense. As former CIA Chief Michael Hayden reportedly remarked, "This is the first attack of a major nature in which a cyber attack was used to effect physical destruction."[2] He likened the transformation in warfare to that which occurred in 1945 with the release of the atomic bomb over Hiroshima. The computer infrastructure of North Korea sustained serious damage, just two days after President Obama warned that the United States would not accept North Korea's threats to attack the infrastructure of Sony pictures unless they cancelled plans to make the movie *The Interview*, intended to portray a CIA plot to kill North Korean President Kim Jong-Un. Sony capitulated and cancelled the movie premiere, much to the consternation of the U.S. government.[3]

Cyberwar, also known as cyberspace operations, is defined by a Department of Defense Memorandum as "[t]he employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace."[4] The Memorandum goes on to say that such operations "include computer network operations and activities to operate and defend the Global Information Grid." As this definition makes clear, the

[1] David E Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, at <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>.

[2] See David E Sanger, *Confront and Conceal* (London: Crown Publishers, 2012), 200.

[3] Soraya N McDonald, "Sony tells theaters they can pass on showing 'The Interview.' Premiere canceled," *Washington Post*, December 17, 2014, at <http://www.washingtonpost.com/news/morning-mix/wp/2014/12/17/sony-tells-theaters-they-can-pass-on-showing-the-interview/>.

[4] Vice Chairman of the Joint Chiefs of Staff, "Memorandum for Chiefs of the Military Services: Joint Terminology for Cyberspace Operations," Washington, November 2010, at James E. Cartwright http://www.defense.gov/bios/biographydetail.aspx?biographyid=138; "Joint Terminology for Cyberspace Operations," in *Cyberwar Resources Guide*, Item #51, at <http://www.projectcyw-d.org/resources/items/show/51> (accessed November 26, 2014).

concept of cyberwar contains an implicit recognition that the US has a security interest in the operation of its electronic network that surpasses the immediate impact of military operations on the protection of human life. Protecting the Grid is comparable to protecting our physical borders: informational security and autonomy have thus become key attributes of national sovereignty.

The importance of defending our electronic infrastructure grows consistently as our dependence on information technology grows. Offensive cyber capacities are of increasing military importance, due to the converse dependence on information technology on the part of our adversaries. At the same time that cyber attacks are providing an increasingly attractive alternative to direct kinetic operations, US and other forces have independently been shifting from kinetic targeting strategies towards more multifaceted approaches, such as those involving diplomacy, economic assistance, education and communications. Cyber operations fit somewhat better with this approach than do traditional kinetic operations. The changing nature of warfare, as well as the changed circumstances in which war takes place, have enhanced the attractions of inflicting the damage of war by non-kinetic means. The methods of cyberwar have thus arrived at a propitious moment.

II. Placing Cyberwar in Historical Context

In 2006, the Department of Defense (DoD) Joint Staff developed a formerly-classified "National Military Strategy for Cyberspace Operations," reflecting a substantially developed and operationally integrated defense cyber capacity. [5] That strategy defined cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures."[6] By 2011, the concept of cyber operations was well enough established that (retired) General Michael Hayden, former Director of the National Security Agency and Central Intelligence Agency, could comment: "[l]ike everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, cyber."[7] However, the seeds of the cyber revolution were sown long before 2011, even prior to the development of computer technology. The techniques of cyberwar are a subset of a broader approach to national defense technology, one that involves the use of the electromagnetic spectrum. The more general category might aptly be called "Electromagnetic Warfare" (EW), of which both cyber and electromagnetic activities are a part.[8]

[5] DoD, "The National Military Strategy for Cyberspace Operations" (2006) 11.

[6] DoD, "The National Military Strategy for Cyberspace Operations" (2006) 11.

[7] Michael V Hayden, "The Future of Things 'Cyber'" (2011) 5 *Strategic Studies Quarterly* 3. By contrast, Libicki's conclusion is very much the opposite:

> [U]nderstanding cyberspace as a warfighting domain is not helpful when it comes to understanding what can and should be done to defend and attack networked systems. To the extent that such a characterization leads strategists and operators to presumptions or conclusions that are not derived from observation and experience, this characterization may well mislead.

Libicki, (n 4) 336.

[8] See Department of the Army, Field Manual (FM) 3-38, Cyber Electromagnetic Activities, February 2014 at <http://fas.org/irp/doddir/army/fm3-38.pdf>.

One of the first uses of the harnessed electromagnetic spectrum for communications in warfare was the telegraph.[9] The telegraph also became the first physical target of EW more than one hundred years prior to the cyber age. By the time of the civil war, 50,000 miles of telegraph cable had been laid for purely military purposes.[10] The telegraph was as much of a revolution in military affairs in the 19th Century as cyberwarfare is in the 21st. Mobile military telegraph wagons sent and received messages behind the front lines all the way to the first President Lincoln's War Department Telegraph Office.[11] Prior to this innovation, the ability to have rapid exchanges between a national leader at the seat of government and his forces in the field had been difficult to impossible. With the telegraph, however, there could be almost instantaneous communication between Washington and armies in distant fields.[12]

The demands on this valuable means of communication led to the first governmental seizure of electronic communications systems. Congressional Act of January 31, 1862 authorized the President to take possession of railroad and telegraph lines if in his judgment public safety so required.[13] Pursuant to this Act, on February 26, 1862, the President seized control of all telegraphic lines, thus laying the ground for executive control of electronic communications and technology as part and parcel of national defense efforts.[14]

By World War I, there was widespread use of wireless radios for civilian communications as well as military transmission of combat information. This was a great advantage, as wireless radios were less susceptible to damage from enemy artillery barrages than were wired telephone lines, and they were not subject to enemy listening by induction.[15] British intelligence was able to crack the code used for messages to and from the German station, and in this way intercepted the infamous German "Zimmerman telegrams" to Mexico, which invited Mexico to attack US territory. Technological advances in espionage had thus uncovered one of the crucial pieces of information that would contribute to bringing America into the war.[16]

By 1916, the British were experimenting with jamming enemy wireless intercept operations, and jamming began along the entire British front in October 1916.[17] Both sides experimented with early efforts at electronic deception, such as false transmissions,

[9] Since the telegraph operates using electrical signals transmitted across wire lines, telegraph operations are electromagnetic in nature, as are radio, telephone, radar, infrared, ultraviolet and other less used sections of the electromagnetic (EM) spectrum. See J B Calvert, *The Electromagnetic Telegraph* (2000), and Tom Wheeler, *Mr. Lincoln's T-Mails: The Untold Story Of How Abraham Lincoln Used The Telegraph To Win The Civil War* (2007)

[10] Daniel W Crofts, Communication Breakdown, New York Times May 21, 2011.

[11] David H. Bates, Lincoln in the Telegraph Office: Recollections of the United States Military Telegraph Corps during the Civil War (1995) ix.

[12] Bates (n 36) x. [13] 12 Stat. 334 (1862).

[14] A concession to private commercial demand for and access to the telegraph was made by the War Department, which articulated that the possession of the telegraph lines was "not intended to interfere in any respect with the ordinary affairs of the companies or with private business." Joshua R. Clark, Emergency Legislation Passed Prior to December, 1917, Collected, Annotated and Indexed Under The Direction of The Attorney General, Current Emergency Legislation 10.

[15] Sterling (n 43) 445 [16] Sterling (n 43) 445.

[17] Comint and Comsec: The Tactics of 1914-1918 – Part II Summer 1972 Vol 2, No. 3 11. The report also notes that "[t]he British soon found that jamming was costly and ineffective and it was discontinued." Comint and Comsec (n 47) 11.

dummy traffic and other similar ruses for misleading the enemy.[18] During World War II, the British began to equip their aircraft with noise jammers and passive electronic countermeasures (ECM) as an effort to foil the sophisticated Wurzburg gun-laying German radars.[19] The Japanese were meanwhile working on their own types of radars, though their efforts were hampered by a dearth of scientists and engineers, as well as by a shortage of materials.[20] Throughout the war, there was a fight between rudimentary EW capabilities and simple ECM,[21] such that each side would temporarily gain the upper hand in EW, only to lose it in a new countermeasure.[22]

It was not until well after the advent of the internet and the attacks of 9/11, however, that the development of cyberwar techniques began in earnest. Although the initial foray in this direction came from the Bush Administration, the biggest support for technological advance has come from the Obama Administration. In 2012, the Administration articulated the National Security Presidential Directive/NSPD-54, which remains the US policy definition for cyberspace.[23] There is now an agency—the Pentagon's Defense Advanced Research Projects Agency (DARPA)—that has the mission of protecting computer systems and developing the capability to disrupt or destroy enemy systems. We are thus transformed, not only in offensive uses of cyber, but also in our attempts to use cyber as a tool for defending against the heavily computer-dependent kinetic attacks of others.

Of course the United States and its allies are not the only world powers that have been developing a cyberwar capacity. In 2007, security firm McAfee estimated that 120 countries had already developed ways to use the internet to target financial markets, government computer systems, and utilities. In 2008, the Russian government allegedly integrated cyber operations into its conflict with Georgia. According to these accusations, Russian cyber intelligence units conducted reconnaissance and infiltrated Georgian military and government networks. When the conventional fighting broke out, Russia used cyberweapons to attack Georgian government and military sites as well as communication installations. Foreign militaries, such as China's, have conducted exercises in offensive cyber operations, both stealing information from other governments and simulating attacks on other countries command and control systems. In 2011, Iran boasted that it had the world's second-largest cyber army. With states around the globe improving their cyberwarfare capabilities, the world may experience a cyber arms race reminiscent of the nuclear arms race of the Cold War.

Arms races revolving around technological advances in war are nothing new, and from experience we know such moments often produce significant changes in the fundamental structure of war. Technological developments have consistently transformed the way wars are conducted as well as the nature of the risks to both combatant and civilian populations. Most notably, increasingly sophisticated and deadlier weapons have enabled combatants to keep a greater distance

[18] See, for example, Andrew Eddowes, The Haversack Ruse, and British Deception Operations in Palestine During World War I (1994)

[19] Peter J. Hugill, Global Communications Since 1844: Geopolitics and Technology (1999) 194

[20] Hugill (n 50) 162. [21] Hugill (n 50) 194. [22] Government of India DRDO (n 33) 14

[23] National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23, Subject: Cybersecurity Policy (U), January 8, 2008 at 3.

from one another, thus diffusing the risks they face. At the same time, such technologies have often broadened the scope of war, further increasing risks to civilian populations. Hayden's comparison between cyber and the transformative power of the new technology reflected in the nuclear attack on Hiroshima seems apt. Less dramatic examples, such as the development of drones, demonstrate the same process.

Precision technologies have increased the distance between combatants at the cost of subjecting civilian populations to new risks in other ways, ironically risks that combatants no longer face. Despite their capacity for precision, mistakes in the use of such weapons have been common, due to inaccurate information, unintended effects on third parties, ranging from death and bodily injury to more diffuse effects, such as the repeated stress from exposure to drones in the vicinity of their targets. Where the use of drones is a persistent feature of everyday life, civilians report symptoms of trauma and anxiety from living in their midst. No technological change to date, however, appears to rival this transformative potential to the same degree as the development of cyber offensive capacities. Indeed, this is captured by the coining of a new label for the notion of war involving cyber attacks, namely "cyberwar," as though it were not only a new kind of weapon, but an entirely new genre of war. The possibility that we might be able to destroy a target like the Iranian nuclear reactor from the "inside out," avoiding detection for significant periods of time while an electronic virus works its way through the system's infrastructure, opens up the possibility of just such a dramatic change in our offensive capabilities. In addition, cyber technology creates the opportunity for a new kind of defense strategy, one designed both to counter cyber offensives and to pre-empt kinetic attacks, under scenarios that do not fit neatly within the traditional paradigm of war. When technological evolution is combined with geopolitical change, such as the demise of state sovereignty and the entrance of civilians or non-governmental actors into the arena of war, the transformative nature of cyber technology is enhanced.

III. Transformations in the Nature of War

The revisionary effect of technological change has conspired with dramatic changes in the basic structure of war, particularly since the United States engaged al-Qaeda in the wake of 9/11. The most significant shift in the demographics of war is the influx of civilians into battle. The US is increasingly drawn into conflict with ideologically driven populations, organized into powerful civilian militias, in lieu of governmental forces carrying out a concerted state policy of old. With this crucial shift in the landscape of war, the formerly bright-line distinction between state and non-state actors has been eclipsed, and with it the boundary distinction between combatants and civilians. However, we cannot satisfy the requirements of the Law of Armed Conflict (LOAC), in particular the crucial principle of distinction, without being able reliably to identify who is a legitimate target. In this way, changes in modern warfare have been attended by a breakdown of the traditional foundation on which adherence to the rule of law in war depends. There is a ripple effect: the widespread entry of civilians into the theater of

war results in a corresponding disintegration of the boundary between military jurisdiction, on the one hand, and the jurisdiction of law enforcement, on the other.

Historically, the distinction between the civilian and combatant populations was a sharp one. The uniform was the most visible means of marking that distinction, but even without uniforms there would have been little doubt about who was military and who civilian. In addition, the civilian population was kept physically separate from war by the fact that the fighting took place on a battlefield, the boundaries of which were fairly clear. In modern conflicts, the historical distinction of roles is no longer applicable, as the enemy consists in non-state actors who blend nearly seamlessly into the civilian population. This is facilitated by the fact that there is no longer a distinct battlefield in war. Military operations now take place anywhere and everywhere. We might indeed say that modern war is characterized by a loss of location and the abolition of the traditional locus of battle, and with the advent of cyberwar we have that process brought to an exteme: cyber represents the complete loss of the physical battlefield. The advent of war in cyberspace is the culmination of that ebbing of historical boundaries around the concept of war.

It is crucial to understand the link between the availability of cyberwar technology and the role of civilians in war. Where the threat to national security comes primarily from non-state actors, it is reasonable to anticipate expanded use of technologies of war where the barriers to entry are low. Such is the case with cyberwar: members of al-Qaeda or ISIS may, in the long run, be particularly likely to turn to cyberweapons to compensate for the kinetic forces they lack. Despite the elaborate effort, planning, and expertise that went into Operation Olympic Games, destructive cyber attacks can be launched with little preparation or expense. Such attacks, potentially carried out by a small number of individuals with sharply limited resources, have the power to impose destruction on a level that only kinetic attacks have hitherto made possible. What enables such destructive capabilities for apparently slight intervention and remote causal impact is the highly technological infrastructure of modern life. We are, in effect, leveraged on technology. The same can be said for civilian life: we are dependent on computers, and breaches of our technological infrastructure can produce devastating results.

A second crucial change in the circumstances of war is the increasing importance of both military and personal data. In an age when individuals voluntarily transmit, store, and receive vast amounts of personal data through the internet, planting software in electronic devices to obliterate, alter, or appropriate data has become a crucial new tactic of warfare: a "fifth dimension battlefield," as it is often said, after air, sea, land and outer space. This shift in frameworks has resulted in the merging of military and corporate espionage functions, and for this reason, the militarization of cyberspace has created a legal and moral ambiguity regarding privacy rights, as well as a personal liability to be targeted in cyberspace by virtue of the mere position one occupies relative to a network of information. These tendencies have contributed to the shift in the structure of warfare, with the result that the line distinction between the military and the civil domains has faded. Cyberwar operations thus occupy a crucial position in the altered landscape of military conflict.

IV. Is Cyberwar an Act of War?

It is often debated whether cyber attacks constitute true acts of war. Those who offer a negative answer to that question maintain that since cyber attacks can cause only limited damage, mostly of an economic nature, such acts do not belong to the domain of war. Those who answer affirmatively maintain the irrelevance of the fact that cyber attacks do not cause physical damage on the grounds that this argument fails to consider the secondary effects of infrastructure failure, particularly where the quality of civilian life is concerned. They point out that one need only recall the loss of life routinely caused by systems failures from electrical surges during fairly routine temperature spikes in the summer months to recognize the destructive potential of cyber attacks.[24] In addition, they argue that the massive damage that cyber attacks can cause, and the serious use of such attacks as an alternative to kinetic attacks in war, belies such claims. Cyberweapons and cyberwarfare are now considered by the FBI to be the number one threat to national security.[25] On the side of the latter position, the US government has taken a functional view of the notion of war and declared cyber attacks as acts of war,[26] given that cyber attacks increasingly serve the function that kinetic attacks have historically served. It therefore becomes harder and harder to see such acts as limited to economic and financial destruction. In response, however, those who reject cyber attacks as acts of war may argue that the point is not that cyber attacks fail to cause destruction, but that the nature of the destruction is unclear. Brown outs are a case in point: while damage from such events may be significant, no one would label them acts of war as a result. Once again, cyber events appear to challenge the traditional categories in war, leaving our theoretical accounts of war in search of an object.

A further difficulty with the functional characterization of cyber attacks as acts of war is that it does not specify the theory of war against which this judgment is being made, and arguably such a theory is necessary in order to know whether a certain characterization of acts of destruction should qualify them as acts of war. Traditional models of warfare are problematic in this regard, since they have all been implicitly called into question by the dramatic changes in the nature of warfare itself. In addition to the advent of cyber attacks and the introduction of other new technologies, there is a fundamental shift in features that formerly characterized acts of war in the first place, and it may seem that the theory of war must evolve as quickly as the emergence of challenging marginal cases whose identity we are seeking to understand by that theory. Because so-called "cyberwar" puts a particular strain on our traditional conception of war, it forces us to return to the basic building blocks of just war theory and to re-examine the theory of war in light of striking new examples.

[24] See the Centers for Disease Control and Prevention website at <http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6231a1.htm>.

[25] See, for example, "FBI: Cyber Attacks—America's Top Terror Threat," *RT.com*, March 2, 2012, at <http://www.rt.com/news/cyber-fbi-security-mueller-691/>; J Nicholas Hoover, "Cyber Attacks Becoming Top Terror Threat, FBI Says," *Informationweek.com*, February 1, 2012, at <http://www.informationweek.com/news/government/security/232600046.

[26] David Sanger and Elisabeth Bulmiller, "Pentagon to Consider Cyberattacks Acts of War," *The New York Times*, May 31, 2012, at <http://www.nytimes.com/2011/06/01/us/politics/01cyber.html>.

Cyber attacks, for example, put immense pressure on conventional notions of sovereignty and the moral and legal doctrines that were developed to regulate them. The problem stems from the fact that the traditional notion of sovereignty and the boundaries of states seem to disintegrate in the face of a type of conflict where boundaries are irrelevant. Could an electronic virus designed to destroy technological infrastructure without ever requiring the kinetic infiltration of the territory or another nation possibly violate the sovereign authority of that other nation? Article 2, Section 4 of the UN Charter promises that members will not use the "threat or use of force against the territorial integrity or political independence of any state." This provision, however, is likely inadequate in view of the increasing use of cyber attacks. It leads to questions of whether problems of cyberwarfare require new treaties and legal definitions. For example, does the cyberweapons race require treaties similar to the Treaty on the Non-Proliferation of Nuclear Weapons? As the country that controls the internet infrastructure, as well as the country with the highest percentage of internet business as a share of its economy, the US is in a uniquely difficult negotiating position in developing any treaties. In a world of attack and destruction without conventional military assets, do traditional notions of sovereignty based on geography and territorial integrity retain their relevance? Unlike past forms of warfare circumscribed by centuries of just war tradition and Law of Armed Conflict (LOAC) prescriptions, cyberwarfare occupies a particularly ambiguous status in the traditions and conventions of the laws of war.

Then there are the difficulties associated with maintaining the principle of distinction. If the threat we are facing stems from the engagement of non-state actors in hostilities, there is little choice but to fight the enemy on civilian territory and in and around the civilian population.[27] This has been one of the most serious developments in warfare since World War II. In cyberwar, however, the difficulty we have demarcating the military and civilian populations in modern warfare is exacerbated. Combatants and civilians are arguably more intertwined than in any other form of war, and, as discussed above, the physical identification of the battlefield, which has helped to mark a conflict as military in nature, has been eliminated. A possible ramification is that efforts to prevent and defend against cyber attacks will result in the complete effacement of the domains of civil and military authority—and, to an even greater degree than exists in modern kinetic warfare, national defense will invade the domain traditionally reserved for law enforcement. If this is true, might military action designed to protect against cyber attacks, for example, pose a serious threat to due process rights, or the moral equivalent of such rights in the international arena? These legal ambiguities, devoid of moral perspective, make adherence to the rule of law in cyberwarfare more challenging than in any other domain of warfare.[28]

V. A Look Ahead

The chapters in this volume grew out of a conference held at the University of Pennsylvania by the Center for Ethics and the Rule of Law (CERL). CERL was founded

[27] Stewart A Baker and Charles J Dunlap Jr, "What is the Role of Lawyers in Cyberwarfare?," *ABA Journal.com*, May 1, 2012, at <http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare>.

[28] Baker and Dunlap Jr, "What is the Role of Lawyers in Cyberwarfare?" (n 8).

in 2012 to address foundational legal and moral issues that arise in national security and modern warfare, particularly those that impact the rule of law. The conference was organized to explore questions about the degree to which engaging in war using the techniques of cyber technology is compatible with rule of law values. The central question was whether cyberwar is consistent with the idea that there are deep moral and legal principles, adherence to which successfully limits the permissibility of war to cases where those principles are observed. Can we both accept the legitimacy of cyberwar and maintain that war is fundamentally a constrained activity, one that can be justified according to a set of moral principles? Or does an acceptance of cyberwar, insofar as it requires us to relinquish our attachment to so many of the doctrines of just war theory, mean that we have given up on the idea that warfare can be limited, in favor of a more Clausewitzian vision that anything goes?

If one does allow that the use of techniques of cyberwar are compatible with the traditional laws of war, and hence with rule of law values, there are further and more fine-grained decisions to be made. One might ask whether the laws of war, such as those typically applied to kinetic war, must be understood as structured in parallel fashion when applied to cyberwar in lieu of conventional techniques of war. Do the laws of armed conflict apply to cyberspace in the same way they apply to traditional warfare?

Proportionality, for example, is a crucial question in military ethics, as well as in domestic criminal law. It requires that no more force be used than is necessary to repel an attack or meet other legitimate military objectives. But how does one determine what constitutes a necessary response to a cyber attack? Worse, how should we determine whether it is *ever* proportionate to launch an offensive cyberwar attack? Was the attack on the Iranian nuclear reactor at Natanz a permissible act of prevention or an illegitimate first strike between sovereign nations? More complicated still, would a cyber attack on the part of the US against North Korea be proportionate to North Korea's threat against Sony pictures?

The current volume brings together leading authorities in law, technology, and moral philosophy, as well as from multiple academic disciplines and representing many types of expertise in practice, to consider the law and morality of cyberwar. We have organized the volume into four parts. Part I contains chapters that attempt to expose foundational and conceptual issues in cyberwar. The chapters in this part primarily seek to answer the question whether acts of cyberwar should count as war according to the criteria of Just War Theory. Larry May's and James Cook's chapters directly contradict one another on this topic: May argues that so-called cyberwar is not in fact a part of the law at all, while Cook maintains that it can be so seamlessly considered a part of the law of war that no adjustment of the Just War Theory paradigm is even required to fit cyberwar in. May's argument draws attention to the aim and outcome of cyber attacks. He argues that insofar as such attacks do not cause, and do not aim to cause, massive loss of life and injury, they are too distant from the types of acts the laws of war have sought to regulate, and so cannot be considered acts of war. May's argument depends on a distinct characterization of war, one we have already identified as necessary if one is to consider whether the laws of war have proper application to cyber attacks. For example, for May, law must be a *public* phenomenon. But since cyber attacks are clandestine, May argues, they do not fit within the characterization of the norms of war that come down

to us through the ages. Thus, May suggests that cyber attacks should be assessed according to the ordinary rules that govern the ethics of conduct in ordinary life, rather than according to the more permissive standard of the rules of war.

James Cook disagrees, and sees traditional Just War Theory as applying as readily to cyber technology as to any other type of attack or initiative in a conflict with another sovereign state. All that is required, Cook maintains, is the ability to identify the agents involved, the intentions with which they act, and the effects of their actions. Hence no revision or updating of Just War Theory is necessary in order to accommodate the central dilemmas of the cyber realm. Rather than argue for this thesis on the grounds that Just War Theory is capacious enough to accommodate the evolving nature of warfare, with cyberwar taking its place at the outer limits of those items to which Just War Theory can rightly apply, Cook reaches his conclusion by asserting the more ordinary nature of cyber attacks and cyberwar activities. Just War Theory applies to cyberwar, then, because there is nothing particularly special to accommodate that conventional war did not already require.

Cook's thesis makes for an interesting contrast with May's, particularly in the characterization of cyberwar itself. While May says that cyberwar is a form of embargo or economic constraint, thus characterizing it as an ordinary form of economic pressure, Cook takes precisely the opposite view. Not only do cyber attacks automatically count as acts of war, given their proximity to kinetic attacks in structure, they are more like war than the standard acts of war that form the paradigm of our treatment of war. Cyber attacks are more potent than other attacks, primarily because once unleashed they require no human intervention to release their potential. Although Cook does not put it this way, a virus like Stuxnet can be fruitfully thought of as a kind of autonomous weapons system, since it functions according to its programming and effectively "takes the human out of the loop."

Jens Ohlin's chapter examining the concept of causation as it applies to cyberwar identifies particular difficulties for the law of war in the context of cyberwar. Although causation is not in general an important concept for understanding the legal limits imposed by IHL, it becomes essential to understand the role of causation where one attempts to understand the limits IHL imposes in the cyber arena. Because cyber attacks are particularly causally complex, it is essential for identifying what Ohlin, following George Fletcher, calls a "pattern of manifest criminality," namely that the rules governing attribution are clear and are able to trace judgments of responsibility along causal lines. The greatest source of complexity lies in the causal role played by third parties, whose involvement may help produce acts and effects that violate the law of war. Until IHL has a more adequate account of causation, particularly as applied to intervening voluntary acts of other agents, it will not be able to clarify the permissibility of cyber interventions under the law of war.

The chapters in the second part of this volume focus on the civil–military divide and the difficulty disentangling these frameworks in the context of cyber security and cyberwar. Stuart Macdonald's paper, which deals with cyberwar and the criminal law, addresses a fundamental aspect of the concept of responsibility as it relates to cyber terrorism. Macdonald's distinction between domestic and enemy criminal law recapitulates the dual framework theories of earlier chapters in its distinction between