Ethics & Cyber Warfare

-Law and Order for a Lawless Frontier-

George Lucas
Visiting Distinguished Professor of Research
John J. Reilly Center for Science, Technology & Values
Notre Dame University

“Where is the Wisdom
Made lost
In information?”

--T. S. Eliot, The Rock (1934)

[forthcoming: Oxford University Press, 2016]
# Table of Contents

Foreword
Preface and Acknowledgements

**Overview: On the Very Idea of “Ethical Cyber Warfare”**

I. Cyber (In)security: Threat Assessment in the Cyber Domain
II. International Law in the Aftermath of Estonia: the Tallinn Manual
III. Is there a Role for “Ethics” in the Cyber Domain?
IV. If Aristotle Waged Cyber War: How International Norms “Emerge”
V. The Cunning of Nature: Just War Theory and Cyber Warfare
VI. Privacy, Anonymity, and the Quest for Cyber Security
VII. Pain and Private Language: the Dilemma of Edward Snowden

Conclusion: “From Navigation, to Aviation, to ‘Cyberation’.” Formulating new “Rules of the Road” for the Information Superhighway.

Endnotes
References
Preface

In a darkened room, in front of several hundred attendees at the University of Pennsylvania Law School in Philadelphia, the deputy director of the National Security Agency displays a Powerpoint slide that portrays an immense, multi-colored map of the world. Generated from the Agency's powerful internet mapping, exploration and analysis program, "TreasureMap," the slide displays thousands of locations across Eastern Europe and the Middle East, from which crippling cyber attacks against virtually every major financial institution in the United States were (apparently) in the process of being launched in the fall of 2012. Are these simply criminal acts, or do they represent acts of war in a new kind of war?

The speaker at the front of the room is Brigadier General Chris Inglis (PhD, USAF Reserve). Invited by Professor Claire Finkelstein, director of the U.Penn Law School's "Center for Ethics and the Rule of Law," he has been approved and dispatched on a round of public speaking by the National Security Agency during the latter part of the year 2013. His

---

1 TreasureMap is described as an interactive, real-time "big-data" collection and analysis tool capable, in principle, of tracking the activities every router, registry, IP address and physical device connected to the World Wide Web: as NSA operatives describe it, "any device, anywhere, all the time." The program was developed by NSA in cooperation with Cisco Systems and information technology experts at the University of California-San Diego. See: https://firstlook.org/theintercept/document/2014/09/14/treasure-map-presentation/. [Accessed 10 July 2015]
appearances (including a lengthy interview and tour of NSA facilities in Ft. Meade, MD on CBS’s news magazine, “60 Minutes”2) are an essential component of the agency’s desperate attempts to give a more favorable public account of its hitherto-classified and secret data collection and analysis activities in the wake of devastating allegations about those clandestine activities, first made in June and July of that year by former NSA contractor, Edward Snowden.

During his brief period of employment in NSA’s signal intelligence (“SIGINT”) station in Hawaii, Snowden had quietly and surreptitiously downloaded massive amounts of classified data documenting the agency's data collection and analysis efforts and findings. He then fled with the stolen data, first to Hong Kong, then to mainland China, and eventually sought political asylum within the Russian Federation in order to avoid capture and arrest by the FBI. He released portions of this information to the Guardian and other news media, charging that the secretive U.S. intelligence agency was engaging in massive cyber espionage, data collection, and surveillance activities throughout the world, including extensive surveillance of American citizens. These revelations and charges stimulated international outrage and concern, evoking images in the public mind of the former East Germany’s feared Stasi (secret police).

Was Snowden engaged in legitimate "whistle-blowing," seeking to inform and protect the American public against government misconduct intended to infringe on their individual liberty and privacy, as he and his supporters maintain? Or was his an act of treason (as angry critics and detractors responded) in the midst of a desperate, ongoing, proactive, and possibly new kind of “preemptive” war of national self-defense?

In the summer of 2010, a German industrial computer security expert, Ralph Langner, reported that a disturbing form of "malware" had apparently burrowed its way into the supervisory control and data acquisitions systems (SCDAS) of large industries in many nations. A subsequent exhaustive examination of this "computer worm" by the internet security firm, Symantec, revealed that the malware was intended to disrupt the normal functioning of the programmable logic controllers (PLCs) that are the basic components of most computer-controlled industrial processes. While the worm (nicknamed "Stuxnet" after portions of

---

Microsoft code that the malware disrupted) had by now been detected in systems all over the world, over 60% of the infected systems were in Iran. Langner and other security experts confirmed that this malicious software was apparently designed to disrupt only very specific targets, and otherwise simply remained dormant and harmless in the remaining systems it had infected (indeed, it had apparently been set to self-destruct in those systems by no later than July 2012!).

As many IT security experts now recognize, this software or "malware" was actually a sophisticated cyber weapon, apparently developed jointly by the U.S. and Israel, as part of a larger clandestine operation known as “Olympic Games.”

3 Stuxnet itself was intended to target the control systems of Siemens nuclear centrifuges, but only a specific array consisting of 984 of one particular model of this company's machines, which happened to be located in the top-secret Natanz nuclear power facility in Iran. Iran was forbidden under international law even to have acquired this embargoed Siemens equipment, which could be used to process fuel for a nuclear weapon. Stuxnet disabled the operation of these centrifuges, causing them mysteriously to spin out of control and sustain serious damage, and all the while send information to their operators that everything was functioning normally.

Prior to its unintended (but evidently foreseen) "escape" from Natanz into the global internet generally (which led to its eventual discovery by Langner and others), this malware seriously degraded Iran's covert nuclear weapons program – according to some estimates at the time, setting the goals of that program back by as much as five years. This was the first known example of a "virtual weapon" in cyberspace causing genuine physical damage in the real world, fully equivalent to what a conventional armed airstrike might have inflicted. But in this instance, there was no accompanying “collateral damage” to other, non-military infrastructure, nor was there any accompanying injury or loss of life.4 Should we regard -- or for that matter, would the

3 For a detailed and authoritative account of "Olympic Games," including the cyber weapons Stuxnet and Duqu, Gauss and the surveillance software Flame, see David E. Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown Books, 2012): 188-225. For an account of what are sometimes labeled these “four amigos,” see David Gilbert, International Business Times (9 August 2012): http://www.ibtimes.co.uk/ gauss-malware-discovered-virus-lebanon-flame-stuxnet-372025. For a brief time following the initial discovery of Stuxnet, these other malware programs, discovered independently, were thought to have been criminal "knock-offs" or copy-cat software produced for non-military purposes by 3rd parties.

4 See the account of this event and its subsequent analysis offered by Peter W. Singer and Allan Friedman in a companion volume in this series, Cybersecurity and Cyberwar: What Everyone Needs to Know (New York: Oxford
Iranian government itself have been justified in regarding – this unmistakable act of military-industrial sabotage as also, in fact, an act of war?

Only three years earlier (in the late spring of 2007), the tiny Baltic nation of Estonia had been the victim of a successive stream of massive "DDoS" ("distributed denial of service") cyber attacks over a three-week period, affecting financial institutions, news organizations, and government agencies throughout that tiny NATO-member nation. DDoS attacks involve a large computer network, or "botnet," generating and transmitting an enormous barrage of messages or logon requests to a specific internet address, overwhelming and effectively "shutting down" whatever agency, organization, or financial service is associated with that address. The attacks appeared to have originated from multiple locations within the neighboring Russian Federation (as well as from some locations inside Estonia itself).[^5]

Only days before the attacks commenced, the Estonian government had reached a controversial decision to move a prominent World War II Russian memorial statue from a central location in the capital city of Tallinn to a somewhat less prestigious location in a nearby military cemetery. Ethnic Russians constitute a sizeable minority (nearly 40%) of Estonia's overall population, and a large majority of them were outraged by this decision. Their subsequent street protests in Estonia were attended by formal diplomatic objections lodged by the Russian government. These were followed closely, in turn, by the cyber massive attacks cited above, which, intermittently for some three weeks in April and May, effectively cut off the country from University Press, 2013): 94-98. In general, I will refer readers unfamiliar with the background concepts invoked in my discussion to consult this excellent companion volume, devoted to the topic of cyber conflict generally.

the rest of the world, and its citizens from their government and financial institutions. The Estonian government, at the time, gave serious consideration to requesting military assistance from NATO under treaty provisions providing for defense and collective security, which would have required characterizing the cyber attacks as the equivalent of a conventional armed attack (a grave step that the perplexed NATO command was unwilling to take).

Then, as suddenly as they began, the cyber attacks ceased. The Russian government consistently disavowed any formal responsibility, claiming they had no control over "patriotic dissidents" within their own borders who might likewise have been outraged by the government's decision. Significantly, no personal injuries or loss of life accompanied the attacks. No physical damage was done to personal or public property or civilian infrastructure, nor were any thefts of financial resources or of personal information subsequently attributed to these attacks. Accordingly, are we to regard them merely as instances of widespread vigilantism carried out by individuals and dissident groups both inside and outside the country, protesting the Estonian government’s actions? Or should we (in agreement with former White House National Security Advisor and cyber expert, Richard A. Clarke, among others) regard the Estonian incident in 2007 instead as the first documented case of "cyber warfare?"6

In contrast, theft of personal information and identify (if not personal property or financial resources directly) was widely reported, and without any doubt the intent of two recent, massive cyber attacks in the U.S.

As this book was being written, in fact, the Director of the U.S. Office of Personnel Management resigned in the wake of revelations of a massive cyber attack on that agency, resulting in the theft of detailed personal information on some 20 million current and former civilian employees in the U.S. Civil Service. The attacks have been attributed with a high degree of certainty to cyber espionage agents of the Peoples’ Liberation Army (PLA) in China. The

---

6 See Richard A Clarke and Robert K. Knake, Cyber War: the Next Threat to National Security and What to do About It. New York: HarperCollins, 2010): 11-16. See also Joel Brenner, America the Vulnerable (New York: Penguin Press, 2011): 127-129. These relatively early accounts have since been extensively amended and the details disputed. While no definitive and uncontroversial account has been offered or accepted, the consensus opinion seems to be that the sort of virtual conflict that occurred in Estonia in 2007 does not rise to the level of a kinetic use of form, or an armed attack, although it likely involved an extensive network of “botnets” operating from numerous locations, so as to defy the interpretation of this being merely the work of one or a few individuals.
intended use of this data, or motives behind the attack (at the time of this writing) were unclear and the subject of much concern and speculation.\(^7\)

That these actions were carried out by highly-proficient Chinese military “cyber warriors,” however, was never seriously in doubt. Indeed, so accurate and reliable has the field of "cyber forensics" now become in only a few short years, that the U.S. was recently able to indict by name five members of the PLA’s now-infamous battalion of cyber warriors, "Shanghai Unit 61384," on “probable cause” for having been responsible for massive cyber thefts of patents and trade secrets from U.S.-based aerospace and defense industries over the past several years, including theft from defense contractor, Lockheed-Martin, of detailed plans and specifications for the U.S. military’s controversial new “strike fighter,” the F-35. The indictments were not expected to result in actual arrest and prosecution of the individuals named, but were intended instead to send a message to the Chinese government that its disavowal or denial of state accountability for these crimes under international law was no longer plausible.

Only a few months earlier, in a widely reported incident during November 2014, North Korean “cyber warriors” apparently hacked into the files of Sony Pictures, Inc., stealing personal information and emails, some of which were released publicly, and others threatened with release, apparently in order to blackmail Sony executives into canceling the pending release of a movie comedy, “The Interview.” The movie portrayed a bungling attempt to assassinate North Korea’s current leader, Kim Jong-un. Never (as was frequently remarked with amusement at the time) had such a lousy movie received such first-class publicity. The entire affair itself seemed almost comic, save for the important principles at stake: the interference by agents of a foreign government in the internal affairs of another sovereign nation, attempting to inhibit freedom of expression, and violating personal privacy on a massive scale for the foreign state’s political purposes. The kind of extortion and blackmail involved, and its impact on corporate and individual behavior in a sovereign country, might not have seemed quite so amusing under

\(^7\) One of the more exasperating features we will encounter in attempting to offer a comprehensive analytical study of such phenomena in this book is that the events under scrutiny occur with astonishing frequency, and interpretations of even the most recent past events are modified or challenged with equal rapidity, rendering it difficult to give a full, fair, and objective account of the events selected for analysis.
different circumstances. The U.S. thus treated this instance of massive, “state-sponsored hacktivism” as a serious act of crime in the context of a wider international conflict.  

But should we now come even further to regard the foregoing two actions, and others like them, when carried out by agents on behalf of nation-states for political reasons, as also the equivalent of military skirmishes in an ongoing cyber war?  

Note that under almost any other circumstances, we would decidedly not regard any of the actions above (with the possible exception of Stuxnet) as something akin to warfare, let alone as equivalent to an act of armed conflict. Indeed, were exactly the same such actions undertaken by individuals or organizations, they would be classified straightforwardly as crimes, many of them very serious crimes, with the individuals involved subject (at least in principle) to apprehension, extradition, arrest, indictment, trial -- and if found guilty, a term of imprisonment. That is how the U.S. and other nations, especially those party to what is known as the CCC -- the (European) Convention on Cyber Crime, formulated by delegates in Bucharest, Rumania in 2001 -- now agree and cooperate in combating cyber crime and cyber criminals today.  

"Hacktivism," for its part, is a recent term of art to classify and describe the individuals and organizations who carry out otherwise-criminal activities (like the Sony Pictures and OPM "hacks") for political purposes rather than personal or financial gain: e.g., to protest government or organizational actions with which they disagree (such as the proposal to relocate the Russian war memorial in Tallinn).  

When nation-states and their agents engage in these sorts of activities, by contrast, we ordinarily classify the activities themselves as constituting espionage.  

---


10 See Singer and Friedman, Cybersecurity and Cyber War, pp. 63-66.

11 I use the term in its original and broadest sense as covering every kind of clandestine activity in the service of the state, including: intelligence, surveillance, kidnapping, “rendition” and interrogation, targeted killing and assassination, sabotage and other covert activities – all carried out by “spies” who are always agents of some nation-state. The term frequently has a more restricted use, limited to surveillance and intelligence-gathering, as opposed to the tasks of “covert operatives,” who carry out the remainder of these activities. Those are subsequent bureaucratic distinctions, however, and not inherent in the original meaning of “espionage.”
covered explicitly under international law, although the individuals engaging in such activities on behalf of their governments are nonetheless subject to arrest and prosecution as criminals (or as traitors, or enemy spies) under the terms of domestic legal jurisdiction within the countries in which their activities are actually carried out. Perhaps, as some critics of the concept of "cyber warfare" itself have objected, this is how we should regard all of the instances above. We should resist (that is to say) confusing or conflating acts of crime or espionage carried out in the virtual cyber domain with acts of war and armed conflict, carried out in the real world.

Cyber warfare, by contrast, is a term that should be reserved to use (if ever at all) only to describe a form of conflict that has been predicted with anxiety, but (again, possibly with the exception of Stuxnet) never actually been carried out...at least yet.

Richard Clarke (in the book cited above) and others of like mind have worried about a conceivable series of cyber attacks -- essentially massive coordinated acts of physical sabotage -- that could be launched against vital and vulnerable civil infrastructure and military installations. Attacks on air and ground traffic control systems would, for example, cause freight trains loaded with chemicals and flammable materials to derail, while planes collided in mid-air or fell to the ground. Electric power grids would be shut down, and hydroelectric generators would (just like the Stuxnet-controlled centrifuges) spin out of control and explode, destroying dams and causing massive flooding and horrific loss of life. Chemical plants would begin to leak poisonous fumes into nearby cities. The resultant “cyber Pearl Harbor,” or “cyber Armageddon,” could conceivably result in widespread death and destruction on the scale of a strategic thermonuclear war. Perhaps most disturbingly, such writers sometimes seem to suggest that massive destruction on such a scale not only could be inflicted by determined nation-state adversaries (like China or the Russian Federation) with immense national resources to invest in the

---

12 Foremost among such critics is a scholar in the Department of War Studies at King’s College, University of London, Professor Thomas C. Rid. See, for example: “Cyber War will Not Take Place,” *Journal of Strategic Studies*, 35, no.1 (October 2011): 5-32, and his most recent book of the same title (Oxford: Oxford University Press, 2013).

13 See Singer and Friedman, pp. 98-100 for discussion of rival definitions of what constitutes cyber warfare. They argue for a more limited and focused definition than is usually employed in the public accounts, but one that is still slightly broader than the very specific and restricted concept I will defend in this book.

development of cyber weapons of their own. Such destruction and havoc could also, at least in principle, be inflicted by a small terrorist cell with only two or three members, or even (perhaps most frighteningly) by your next-door neighbor’s alienated 14-year-old, laboring in isolation and secrecy in his upstairs bedroom.

Cyber warfare itself is a term first coined in the 1990s by a renowned international and strategic studies expert at the Rand Corporation, John Arquilla, in discussing the prospects for what he, and the eminent Georgetown University computer scientist, Dorothy Denning, also termed “information warfare.”15 Their warnings met with skepticism at the time. But fellow Rand Corporation scholar, Martin C. Libicki, has since offered some of the most detailed and plausible analysis of what the actual threat levels of such warfare are now, and might soon become, as well as how we might secure ourselves against this threat.16

Such anxiety-provoking predictions have abounded for more than a decade. Yet again, with the possible exception of Stuxnet, the scenarios predicted have not actually occurred (once again, more accurately: at least not yet). For my own part, I have maintained during this same period that the threat posed by the teen-age neighbor, or the terrorist cell, at least, are likely exaggerated. To wage a genuine “cyber war,” an individual would need to be more than a very clever and unscrupulous, alienated computer geek. The individual would require access to a hydroelectric generator on which to practice and extensively test the design of the controlling software, for one thing. And (as I have repeatedly stressed to numerous audiences around the world whom I have addressed on this topic)17 it can prove rather difficult to gain access to such equipment, let alone wrestle a large hydroelectric generator up the steps and into the third-floor


17 French Military Academy in Saint-Cyr, CREC Paris conf, FIC annual symposium in Europe (2013), ANU Defence College Canberra (2014), Monash University, as well as Yale University, Naval War College, and I delivery of annuStutt and McDermott lectures at USNA and USAFA, respectively (to name but a few).
terrorists’ flat in Hamburg. Likewise, such a device does not fit neatly into the upstairs bedroom of your neighbor’s son who (having likely deliberately ignored and flunked his physics and engineering courses in order to experiment on his computer) probably wouldn’t begin to know what to do with it anyway.

Genuine “cyber weapons,” that is to say, consist exclusively of complex software designed to exploit vulnerabilities in other software, such as the Windows operating system used on most computers, or the industrial control systems (ICAs) that govern the operation of industrial devices and processes throughout the world. This requires knowledge, not just of how to code software, design destructive virus programs, and engage in mischief and crime – but also demands that the designers have extensive knowledge of how their intended “targets” (these vastly varied industrial machines and systems themselves) actually operate. And beyond this, the design of the proposed cyber weapon requires years of planning and practice. The software weapons may, for example, emulate the normal operation of an array of equipment at a factory or energy company, while simultaneously taking control of, and destroying the equipment itself, or disrupting the processes it controls (such as the flow of oil through a pipeline, or of electricity across a power grid). All this requires a range of knowledge, experience, expertise, and physical resources on which to practice and test weapons designs that far exceed those of any typical individual, or even the most dedicated and well-resourced criminal or terrorist group.

Contrary to Professor Thomas Rid’s blanket dismissal of all such prospects that I cited above, however, the hypothetical threat of determined adversary nations engaging in something like what the foregoing experts in information technology have described as genuine “warfare” in the cyber domain remains a plausible threat (even though nothing full-fledged along the lines of these frightening scenarios has yet transpired). Surely Stuxnet demonstrates that. Hence, how seriously should we take this threat, and what might we be entitled to do in order to respond to it?

That question regarding the price of cyber security constitutes an important topic discussed in this book. Even more significantly, this book is intended to examine what has actually happened in the absence of something recognizably like authentic warfare in the cyber

domain -- something many experts and colleagues have begun to describe as an altogether new kind of warfare: “soft” war, or “unarmed conflict.”

That is to say: if we set the interesting case of Stuxnet aside for the moment, all of the other examples of conflict in the cyber domain – examples about which Rid and I seem to agree on as comprising crime, vandalism, vigilantism and espionage – have trended in a very different direction than those earlier cyber experts like Arquilla and Clarke anticipated. Rather than empowering individuals (or terrorist groups) to wreak havoc in the cyber domain on the scale of conventional kinetic war carried out by nation-states, instead we have increasingly witnessed states like North Korea, China, and Russia (and perhaps the U.S., U.K., Australia and other allies as well) behaving more and more like individuals.

What I will try to document in this book is that states have increasingly engaged in “soft” or “unarmed” conflict with one another that differs from the kind of low-intensity conflict traditionally associated with espionage. As in the Sony-North Korean case, the states are behaving more and more like alienated teen-age “hackers,” carrying out crimes of petty vandalism, theft, disruption, destruction and even cyber-bullying, for political purposes.

Nations are also increasingly behaving like non-state vigilante groups, such as Anonymous: i.e., just like the members of that loosely-organized internet vigilante group, states themselves are randomly attacking the internet property, vital information, essential activities or other valuable organizational resources of those with whom they violently disagree, while engaging in threats, extortion, and blackmail.

And though each individual action might formally constitute a crime, the overall strategy or intentionality differs markedly from straightforward criminal activity, in that these actions by states are not carried out for individual financial gain or other personal, self-interested motives. Instead, these otherwise-criminal activities are explicitly intended (as Clausewitz described the intention of warfare itself) to impose the cyber aggressor’s political will upon its adversaries through non-political means. These actions differ in scope and also frequently in kind from

---

20 See P. W. Singer and Allan Friedman, Cybersecurity and Cyberwar, pp. 66-69 for an account of the growth and composition of “Anonymous.”
conventional espionage. Or perhaps these activities indicate *a dramatic new evolution in the practice of espionage itself* toward a more public and dominant role in international relations than its former subsidiary role of merely gathering and using information about adversaries to gain a material advantage for the sake of national security. Instead, once again – just as in the classical, Clausewitzian description of warfare – all of these activities in cyber space are carried out for explicit purposes of political domination: i.e., in order to force the political goals and aspirations of the aggressor upon the victim.

I call this “*state-sponsored hacktivism,*” and it -- rather than the earlier predictions of conventional, effects-based warfare carried out with sophisticated cyber weapons -- seems to be the way international relations and inter-state conflict are evolving in the present. It seems quite reasonable to regard all this as constituting a *revolutionary new kind of warfare, unrestricted in scope and duration, and carried out without regard for existing international law or the customary ethical norms of state behavior* governing the conduct of conventional inter-state conflict. Like the earlier rise to prominence of terrorism and non-state-based insurgencies that has come to be called "irregular" warfare, these activities by states themselves in the cyber domain seem to represent a novel and highly "irregular" or non-customary mode of engaging in conflict and domination. This is ongoing, unrestricted warfare – warfare without rules, a “war of all against all,” carried out in a domain resembling Thomas Hobbes’ hypothetical state of nature, in which the rule of law has thus far been actively repudiated and resisted by the “citizens” or “inhabitants” of this novel domain.

How should we come to terms with this new development? How, in particular, does it affect our notions concerning warfare and state-sponsored conflict in general? And most especially, how does it affect (I would say, “transform”) the debate about whether there is now, or ever could be, something properly called cyber warfare? These are among the important topics this book will address.

For the moment, let us return to the “TreasureMap” slide with which we began. The deputy director of NSA was engaging in public outreach and massive "damage control" in the aftermath of Snowden’s leaks of classified information on the agency's “big data” collection and surveillance activities. *What does all this have to do with cyber warfare?* All those much publicized events and developments instead pertained (did they not?) to something else entirely:
namely, to government (mis)conduct and the prospective erosion of individual rights and personal privacy. Certainly that is what Snowden and his supporters contended in justifying his actions, and in attempting to classify them as “whistle-blowing” directed against the government’s ever-increasing infringement of individual liberty.

But the global interactive map in that PowerPoint slide shown in response appeared to illustrate a massive cyber attack in progress, originating from thousands of nodes or sites throughout Europe and the Middle East. That, in turn, suggested a massive criminal network, engaged in some kind of financial theft or fraud, since U.S. banks and financial institutions were the apparent target.

But not so. It was all “spoofed.” These attacks, in the fall of 2012, originated in fact from one masked site, apparently inside Iran. The group that eventually claimed credit for the attacks, when their origin was revealed, described themselves as the “Cyber Fighters of Izz ad-Din al-Qassam” [مقاتلون السيبراني عز الدين القسام].

And who are the Cyber Fighters of Izz al-Din al-Qassam? They appear to be an organization taking its name from a prominent early 20th-century Muslim cleric and anti-colonialist. In 2012, on the anniversary of the “9/11” terrorist attacks in the U.S., this group claimed to have carried out the massive DDoS attacks on U.S. financial institutions that NSA’s deputy director had portrayed. The attacks were then described in a Twitter post by the group as having been launched in retaliation for the continued presence on YouTube of the American-made film, “The Innocence of Muslims.” That piece of hate-mongering propaganda, in turn, portrays Islam, and the prophet Mohammed himself, in a very scandalous and unflattering light. The “Cyber Fighters of Izz al-Din al-Qassam” vowed to continue their attacks until the U.S. President ordered the offending film removed from the Internet.

Two things stood out regarding what were described, at the time, as the most serious and disruptive attacks on American financial institutions ever carried out. First, despite its claim of independence, the group’s attack was not altogether indiscriminate. The specific institutions actually targeted were primarily those that had complied with the terms of the ongoing U.S. economic sanctions against Iran, which were, in turn, part of the international effort to halt that nation’s nuclear arms program. In particular, the group’s demand that a film be censored on
account of its political or religious content seemed hollow: their leaders had to know that this was a demand that was beyond the power of a democratic government or its leaders anywhere to grant, even were they willing in principle to comply with such a demand.

The second oddity was that the anonymous Twitter site from which this group issued its September 2012 proclamation turned out to be the same account from which messages had flowed a few weeks earlier (allegedly from another vigilante group entirely) in the aftermath of a massive cyber attack on the internal computer network of ARAMCO, the Saudi Arabian oil giant. Those attacks, on 15 August 2012, allegedly carried out by an organization calling itself the “Cutting Sword of Justice” [قطع السيف الاصلد], erased data on all affected computer drives, and inserted in their place the image of a burning American flag.

U.S. security officials seemed quite certain in the final analysis that both of these attacks constituted acts of retaliation by Iranian state agents, rather than some anonymous Islamic vigilante group. And these attacks were directly in response to the damage done to Iran’s own nuclear and oil infrastructure by “Stuxnet” and “Flame,” respectively, both weapons attributed to (but never acknowledged by) the U.S. and Israeli governments. Strike, and counter-strike. Attack and retaliation. The National Security Agency, it turns out, had been engaged in countering attacks against our financial infrastructure by an adversary nation. The tools of the NSA’s so-called "Enterprise Knowledge System" that Snowden revealed to the public, including the much-ballyhooed "X-keystroke," that gargantuan "Mainway" database in Utah, PRiSM and "TreasureMap," were all tools or weapons being deployed in a war of national self-defense.21

This constitutes the reality of “state-sponsored hacktivism.” And this, I maintain, is the new face of warfare in the 21st century.

---

Overview

On the Very Idea of “Ethics” and Cyber Warfare

A book proposing to discuss “the ethics of cyber warfare” seems all but doomed to failure at the outset. This is because, for one thing, few agree and what cyber warfare is, while many persons hold deeply contrasting and incompatible views about “ethics” – both about what it even is, let alone about whether it has any relevance or application to conflict and competition in international affairs.

As we have just seen, there is no widespread agreement on whether there even is such a thing as cyber “warfare,” let alone on what it might actually be like. Toward a resolution of that problem, I will propose in this book that “Stuxnet,” at minimum, constituted an example of a skirmish in one authentic and justifiable conception of what “cyber warfare” might be like. This first conception falls within the boundaries envisioned by some of the leading authorities who have warned of the risks of what they describe as conventional, “effects-based” cyber conflict, something to be regarded as equivalent to regular or conventional warfare, but carried out with cyber weapons.

But I will also set forth an altogether different conception of cyber warfare, distinct from the kind envisioned in those earlier prognostications. The “cyber warfare” I will describe resembles somewhat more the cyber-equivalent of “irregular” warfare in the real world, which is itself a kind of armed conflict that has currently all but displaced notions of conventional warfare as Carl von Clausewitz envisioned it.

In this book devoted to conflict in the cyber domain, I will maintain that not only has this new type of “virtual” conflict blurred the distinctions between conventional low-intensity conflict (like espionage) and the “kinetic” or high-intensity conflict characteristic of conventional war. It has also inverted the command and power structures involved in waging war itself – indeed, turned everything “topsy-turvy.” Where once upon a time, for example, the organizations and personnel involved in intelligence and espionage served the broader strategic purposes of the conventional war command structure to which they were wholly subordinate, now it is the leaders of the intelligence and espionage communities (both military and civilian) who “call the shots,” determine the strategy, and establish the parameters of conduct for cyber
conflict. Conventional warriors threaten to be shouldered aside by a new generation of “cyber warriors.”

Something like an equivalent “personnel and leadership transformation” has also transpired over the past two decades in the midst of “irregular warfare” as well. “Drone” pilots and Special Forces have gradually supplanted and increasingly even replaced the activities of conventional air and ground forces. There is much to be learned from that earlier and ongoing internal transformation of military professionalism and combat leadership now, as we turn to the topic of cyber warfare.

But, as I have argued at length elsewhere, perhaps the most significant new feature peculiar to cyber conflict alone stems from a deep-seated anthropological distinction between “warriors” and “spies.” Conventional combatants are required to be familiar with the customary “professional” (internal, ethical) and legal (external) constraints on their conduct of armed hostilities, even if those are on occasion violated, ignored, or otherwise held in contempt. By

---


contrast, there are no “external” constraints to hold in contempt within the world of espionage, where intelligence-gathering and analysis routinely “target” civilians as well as military personnel, and regardless, almost always (as we noted above) constitute criminal behavior within the specific jurisdictions in which those espionage activities take place. These features invariably lead to the inaccurate belief that clandestine agents can do whatever they want to whomever they wish, if circumstances and national interests so dictate.

There are somewhat poorly or vaguely understood personal and “professional” constraints that constitute the relatively nascent field of “intelligence ethics” concerning, for example, duties of loyalty owed to assets and allies in foreign countries, limitations on the types of deception that might be practiced under a given set of circumstances, respect for the privacy and property of ordinary citizens, and so forth. And most intelligence organizations in democratic countries, in point of fact, answer to a domestic legal regime of accountability and oversight, together with an established organizational hierarchy governing covert operations. (The robustness and effectiveness of these means of oversight and accountability are matters that received intense scrutiny in the aftermath of the Snowden affair in the U.S.)

But whatever those “internal” personal and professional constraints are, or how well or poorly they are understood, the important fact we will examine is that their content is substantially different from that attendant upon conventional military and combat personnel. There is, as yet, nothing like a “code of the warrior,” or a “law of armed conflict” equivalent

---

24 See, for example: *The Ethics of Spying: A Reader for Intelligence Professionals*, Vol. 2, ed. Jan Goldman (Lanham, MD: Scarecrow Press/Rowman & Littlefield, 2009), and Goldman’s earlier path-breaking collection in Vol. 1 (2005). See also David Perry, *Partly Cloudy: Ethics in War, Espionage, Covert Action and Interrogation* (Lanham, MD: Scarecrow Press/Rowman & Littlefield, 2009); and James M. Olson, *Fair Play: the Moral Dilemmas of Spying* (Washington, DC: Potomac Books, 2006). Goldman is also founder and editor of the *International Journal of Intelligence Ethics* (IJIE), a peer-reviewed journal now in its fourth volume. None of these works, nor past issues of the journal, have yet addressed topics like “ethics for cyber warriors,” or the fallout from the Snowden affair, but will inevitably do so in due course.

for cyber warriors. How might this profound cultural difference come into play when formulating a national security strategy, let alone in carrying it out, in the cyber domain?26

A second problem we face in this book, however, is that even if we could argue plausibly that there is such a thing as cyber “warfare,” which we have already experienced, or might one day come to experience – still, on any of the many descriptions of what it might be or look like considered above, it would not appear hopeful that "ethics" would ever come to play a significant role in such conflict. Doesn’t the concept of "unrestricted warfare," in particular, entail a war without rules, constraints, or restrictions? And indeed, hasn’t a major problem encountered with “irregular” warfare, insurgency, terrorism, and counter-terrorism in the real world during the past decades confronted us with a similar dilemma of appearing to advocate “war without rules?”

Third and finally: were it not enough simply that cyber conflict, and the concept of “cyber war” specifically, are inchoate and subject to widely variant understandings and interpretations, the topic of “ethics” (especially when applied to interstate conflict) is even more so. Just as with “cyber warfare” itself, there is likewise no widespread, let alone universal agreement on what constitutes “ethics” or morality, despite the determined efforts of moral philosophers to demonstrate otherwise.

Indeed, the subject matter of moral philosophy (my own field of interest) suffers from an enormous degree of public skepticism, in a rather unusual and puzzling fashion.

On one hand, most people worry about "morality" (often about its perceived erosion in social life), for example, and strive themselves to inculcate or practice what they believe to be "ethical behavior." Yet, on the other hand, those very same people are likely simultaneously to admit that understandings of these moral ideals and guiding principles vary widely among individuals and cultures, as well as between different practices or professions (business, versus health care or the military, for example), or else stem from roots in religious beliefs that themselves vary enormously among individuals and cultures.

26 This interesting and problematic “cultural inversion” is discussed in clear laymen’s terminology in a recent issue of The Economist, where similar points are made concerning the ascendancy over, and the impact of the accompanying transformation of espionage with respect to, conventional armed conflict. See “A New War of Espionage,” (1-7 August 2015): 53-54, preceded by the provocative note on “What Laws in the Jungle” (p. 13).
Hence, apart from grounding their own morality either in personal beliefs (drawn perhaps from their particular religious convictions), or else in the moral values they may believe to be enshrined in domestic law within their own particular jurisdictions, they have no broader understanding or justification for the seriousness they might otherwise sincerely attach to the importance of moral principles and sound ethical behavior. And such deeply ingrained cultural and legal relativism can hardly serve them, or anyone, as an effective guide to appropriate conduct in the brand-new realm of cyber conflict, where “privacy and liberty” have come to be equated with “anonymity” and an utter lack of accountability, and within which the sole reigning belief system appears to be, “each cyber citizen can and should do whatever she or he pleases, without fear of consequences.”

And, once again, notwithstanding their own personal convictions about the importance of personal moral rectitude, individuals are often convinced at the very same time that “ethics” has no place in international relations generally (as Machiavelli and Clausewitz seemed to argue), and is, even more, a patently ridiculous or self-contradictory concept when it comes to war and armed conflict (which straightforwardly involve illegal and immoral things like “killing people and breaking things”).

Perhaps this is why no author has yet attempted to write a book about the "ethics" of "cyber warfare." And perhaps also this is why, when I then first proposed to do so, friends, critics, publishers, and their anonymous referees all replied, in effect, “well, good luck with that!”

To be sure, there are plenty of books devoted to the description, analysis, and policy implications of cyber conflict and information warfare. Some of these -- e.g., a work by Jeffrey Carr, together with an excellent introductory survey by Peter Singer and Allan Friedman (listed in the concluding “References” section), as well as those now-classic accounts by authors like Clarke, Brenner, Arquilla and Libicki cited above -- do invoke ethical and legal concerns alongside policy considerations.\(^{27}\) Likewise, there has been a good deal of attention paid to

\(^{27}\) So closely did the design and deployment patterns of “Stuxnet,” in particular, follow the ethical principles for cyber conflict first laid out more than a decade ago in the earliest articles of John Arquilla that, when the worm and its precise mode of operation were finally made public, I mentioned to him that its designers (whoever they were) must have read his work! See: “Just War Doctrine and Cyber Conflict,” 12th Annual Stutt Ethics Lecture, U.S. Naval
ethics and cyber conflict, by a plethora of distinguished and highly accomplished scholars -- such as Randall Dipert in moral philosophy, or Michael Schmitt in the field of international law of armed conflict -- writing in peer reviewed academic journals, or contributing chapters to anthologies which are themselves devoted wholly or at least in part to the topic of ethics in cyber conflict. Most recently, a constellation of bright new stars has arisen in the horizon, thoughtful young scholars and policy analysts like Patrick Lin, Adam Henschke, Heather Roff Perkins, Fritz Allhoff, Ryan Jenkins and B.J. Strawser (to name only a few), who have published important essays, organized international symposia, and edited anthologies of important articles devoted to the ethics of cyber warfare. These, too, occupy a place of prominence in the references listed at the conclusion of this book. I am deeply beholden to these earlier efforts, and will draw extensively upon the many insights into this complex topic that those previous books, articles, and authors have provided.

But heretofore there has been no broad or foundational attempt by a single author to offer an inclusive or comprehensive and systematic perspective on this topic (which is what a book, as opposed to an article or a collected anthology of articles, seeks to accomplish). Indeed, as we have witnessed, there are legitimate questions about whether a systematic and coherent approach to ethics and cyber warfare is even possible, let alone worth undertaking.

Certainly I agree that it would be difficult for any one individual to pretend to possess the requisite comprehensive expertise in all the fields of information technology, computer science, or in political science, international relations, or international law that would be necessary to write an original treatise on this topic. I do believe, however, it is time that someone with a synoptic view of the field attempt to draw together systematically all the various, multidisciplinary threads of discussion, and to recognize (and to respectfully and critically synthesize) the enormous contributions of many of the leading international scholars who have contributed to the discussion of cyber conflict, as well as to the possible role of ethics or the rule of law proposing to govern it. This is especially urgent, as we will discover, on account of the wildly

---

disparate accounts even of the largely indisputable facts surrounding cyber conflict, let alone of their proper interpretation.

By far the most substantial contributions to discussing the governance of cyber conflict have come in the field of international law. Early on in the advent of cyber conflict itself, and with special urgency after the Estonian cyber attacks of July 2007, leading figures in international law from around the world – Michael Schmitt, Scott Shackelford, Duncan Hollister, David Graham, Major General Charles Dunlap (USAF, retired), to name only some of the most prominent – offered significant interpretations of existing international law (both criminal law and the law of armed conflict, or “humanitarian” law) in an attempt to understand both the law’s “reach” and its potential for jurisdictional authority within the cyber domain. The most important document arising from this widespread concern and international collaboration among some of the world’s leading legal scholars is the so-called “Tallinn Manual” of 2012, attempting to illustrate how existing international law can be interpreted and extrapolated to the governance of these new and novel forms of conflict. That is potentially very significant indeed, since there appears to be little appetite within the international community for adopting any further new “black-letter” legislation or treaties to govern the cyber domain.

Accordingly, I propose to give full and careful attention to the contributions and enhanced understanding of the rule of law arising from this impressive collaboration. In the process, however, I will raise serious questions about the relevance, adequacy, and applicability of those results, and more generally, of relying on existing international law alone to address all the morally salient features of cyber conflict (whether above or below the threshold equivalent to an “armed attack”). Specifically, I present concerns about jurisdiction: about, for example, whether laws and legal conceptions concerning conventional armed conflict can, in point of legal fact, be legitimately interpreted to cover kinds of conflict that they were never specifically nor explicitly intended by their framers to address, especially forms of “low-intensity” conflict which (like espionage itself) have been traditionally understood to lie beyond the reach of international law in particular. That will continue to be problematic, even in light of the proposal by the

---

“International Group of Experts” to extend their discussions very soon to other, possibly-relevant bodies of international law beyond the law of armed conflict, such as the law of the sea, space law, and international telecommunications law (as well as human rights law and the law of State responsibility).

This, in turn, will raise some further concerns, both familiar and somewhat unfamiliar, about what is termed the “normative force” of the law itself, as well as calling attention to a fundamental equivocation within international law regarding the kinds of “entities” thought to be the proper subjects of governance under such law.

“Normative force,” for example, pertains to the power that the law has, both to encourage proper behavior and punish infractions. International legal scholars likewise frequently equivocate on this important conception as well. On one hand, they will describe international law as reflecting what states themselves either do, or tolerate being done. That conception is often referred to as ius gentium, or customary law, and it possesses little in the way of “normative force” if states choose to override it, or tolerate others doing so. On the other hand, they (like most of us) also believe that the law defines and prohibits certain forms of unacceptable conduct, such as genocide and other basic violations of human rights, and that it is founded upon fundamental inviolable principles (like state sovereignty and territorial integrity) that are not to be transgressed, no matter what states themselves do, or tolerate being done in such matters. It is difficult to hold or reconcile such contrasting views coherently and consistently.

Finally, I shall raise some serious political questions about what might be termed the “Tallinn process” itself: i.e., the manner by which the so-called “International Group of Experts” was constituted, and their findings formulated, adopted and promulgated. I will argue that the underlying methodology was both insufficiently inter-disciplinary (excluding important kinds of relevant stakeholder expertise) and, even more importantly, insufficiently inclusive from a global political standpoint. The collaborators were, in particular, insufficiently familiar with both the practices, and with the interests of the practitioners (including adversary nations engaged in cyber conflict and possibly in authentic cyber warfare) whose conduct the law seeks to govern. In this they, in essence, presupposed what they were assembled to demonstrate and justify: that
international law properly has jurisdiction in these affairs (something that the Chinese government, for example, has explicitly repudiated regarding activities in cyberspace).

In this important political sense, the Tallinn process itself failed to recognize the most basic and salient features of what is termed in jurisprudence, “good governance.”29 Thus far, as a result, the Manuel has failed to attain anything like widespread acceptance within the international community beyond the immediate NATO constituency from which its expertise was drawn.30

Ethics and the Law are simply not identical topics, despite the tendency often to collapse the subject matter of one into the other, or (even more mistakenly) to hold that Law alone is finally the bedrock concept pertaining to the appropriate norms of human behavior. Quite the contrary, when Law fails to address important new conflicts and conundrums explicitly, it is necessary to resort to Ethics in order to sort things out: to discern, for example, underlying principles of law and jurisprudence that might be invoked (in the absence of bright-line statutes, treaties, or precedent) to guide our insights and intuitions into how to best confront the controversy in question.31

29 Canons of “good governance” as applied to control of emerging military technologies generally (including cyber conflict) are discussed at length by an experienced international lawyer and legal scholar at Rutgers University, Brigadier General Richard M. O’Meara, Ph.D (U.S. Army, retired) in a fascinating and lively study, Governing Military Technologies in the 21st Century: Ethics and Operations (New York: Palgrave-Macmillan, 2014). O’Meara, a former Army IG and Vietnam combat veteran, led the strenuous opposition by military lawyers in 2004 against the U.S. government’s approval of torture and prisoner abuse as acceptable forms of “enhanced interrogation.” It is his account of what he terms “the canons of good governance” upon which my treatment relies in this book. Also enlightening is the editor’s opening chapter on morality and law in: Normative Pluralism and International Law: Exploring Global Governance, eds Jan Klabbers and Tuoko Piiparinin (Cambridge: Cambridge University Press, 2014): 1-33.

30 I first encountered this sweeping characterization of its impact, as (in the words of one senior staff person) “a spectacular failure,” emanating from U.N. and ICRC experts meeting at ICRC headquarters in Geneva in May of 2013, came as a stunning surprise and disappointment. I had assumed without question that the findings of the Tallinn Manual would, almost without question, prove definitive and authoritative, as I discuss at greater length in Chapter Two.

31 On the point of applying law and morality to the governance of cyber conflict, for example, a gifted young colleague practicing international law for the U.N. in Geneva writes: “the comparison [of cyber conflict] to ‘irregular warfare’ ... draws attention to a few well known problematics, namely, the fact that these fall ‘outside’ most legal norms that have been developed for conventional inter-state conflicts. When states engage more and more in ‘hacktivism’, moreover, attribution becomes extremely difficult, and hence, [so does] enforcement of the law (even if it were clear) ... and that, in turn, is because] the relationship between law and morals is indeed a very entangled one. Both are conceptually distinct frameworks of investigation - and depending on what kind of question one seeks to answer admitting or denying a relation might be appropriate. The connection between law and morals, however, can never simply be affirmed or denied in
All that said, considerations of the "ethics" of cyber warfare, in contrast to the extensive legal discussions cited above, came along (with a few exceptions) relatively late in the evolution of cyber conflict itself. The preliminary ruminations of some early writers on “information warfare” (such as Arquilla and Denning) did indeed cite ethical concerns, but their authors were not themselves specialists in this field. As a result, they tended to invoke both the presumed authority and the summary findings of this field (such as classical “just war” theory) somewhat literally and uncritically, leaving open the question, for example, of why other individuals or governments contemptuous of "just war" doctrine should take their concerns or prescriptions seriously.

The first bona fide moral philosopher to take on this task was Professor Randall Dipert of the University of Buffalo -- a philosopher, game-theorist and mathematician, and technical cyber expert -- in a path-breaking essay entitled (like this book) simply, “The Ethics of Cyber Warfare.”\(^{32}\) His work has proven both enlightening, and highly influential, and I shall accordingly attend to his findings seriously.

I will take serious issue only with one underlying observation made body of work: namely, that the features of objects and events in the cyber domain are so unique, and so utterly disanalogous to anything encountered in the everyday physical world, as to obviate both the relevance or applicability of either international law, or of its underlying moral foundation in a

---

absolute terms as it always depends on what it is you are trying to argue. For example, if one seeks to authoritatively answer whether certain acts in cyberspace are 'wrong' one can do so by either moral, ethical, or legal standards. Because law aspires to be in harmony with the values of its subjects' community, one will ideally find the 'same' answer. One can, however, not determine whether something is legal, by providing moral or ethical arguments - even though one can invoke such arguments in order to determine whether something should be illegal (i.e. arguing for the development of new rules). Technological innovation in general enhances human capability and makes things possible that weren't before. For this reason it may appear that existing rules and regulation may no longer appropriately govern, i.e. outlaw undesirable behavior. In order to identify what 'undesirable' behavior is, it is no longer sufficient to turn to the law, but one may answer this question in relation to the values which the law claims to protect, but apparently no longer does.” (Elena Finckh, United Nations Disarmament Information and Research Institute (Geneva), personal correspondence of 24 July and 2 August, 2015).

\(^{32}\) See: *Journal of Military Ethics* 9, no. 4 (December 2010), 384-410. Dipert is, without question, the leading authority in this field, and one of the few to possess nearly all the qualifications I cited as requisite for writing a book like this, and it is unfortunate that it is not he (rather than me) who is author of the present work. What he has done instead is publish widely in scholarly and academic journals since on this topic, as well as contribute to each of the recent important anthologies on ethics and cyber warfare to which I call attention, below. These numerous seminal works are collected in the References section at the end of this book, and cited and drawn on as appropriate throughout this work.
body of ethical precepts known as the “just war tradition” (or sometimes, as above: “just war
theory”). Both, Dipert claims, have no ability to adjudicate conflict in the cyber domain.

Such claims regarding the presumed irrelevance of just war theory and the law of armed
conflict to cyber war and weapons were, in fact, frequently offered over the past decade. Such
assertions were, likewise, frequently offered in the early days of “irregular” warfare, including
even humanitarian military intervention. In both instances, the rapid appearance and
transformative effects of the new practices tempted nearly everyone initially to conclude that
these were “game-changers,” and that all bets were off concerning the adequacy of existing law,
or traditional forms of moral or legal reasoning, to cope with the new regime. In both instances,
however, such concerns have proven (or, I firmly believe, will be proven) to be unfounded.

Rather, the question (already definitively addressed by the NATO group of eminent
international scholars convened by Michael Schmitt in the case of the law) is not whether, but
how the law of armed conflict (as well as international criminal law, and other legal regimes,
such as space law or law of the sea) can be interpreted to apply to these new and somewhat novel
circumstances. This is also the present challenge faced by what is conventionally termed “just
war theory” (JWT) in ethics: it must likewise be able to demonstrate its continuing relevance
and applicability to conflict in the cyber domain. The ethics challenge is an important one to
address, should it turn out (as I aver above) that there may yet be elements of cyber conflict that
“fall through the cracks” of international humanitarian law, on any re-interpretation. We will
likely discover that we urgently require the normative insights of both sources of guidance and
governance of conduct in this new domain.

The initial problem for JWT, however, is every bit as acute and perplexing as that posed
earlier for international law: namely, if there is no such thing as “cyber warfare” – or, if what
we tend to call “warfare” in the cyber domain is, in reality, something else altogether – then how
can the lengthy historical tradition of moral reasoning pertaining to conventional warfare be

33 Just war “theory,” or the “just war tradition” (JWT) is the name conventionally given to a centuries-long
discussion in Western moral philosophy, from Plato, Cicero, St. Augustine and St. Thomas Aquinas, all the way to
Kant, Mill, and contemporary political philosophers like Michael Walzer and John Rawls, regarding when, if ever,
the resort to force is justified, and discussing the proper conduct of the resulting armed conflict, in international
relations. We will return to this topic in great detail later in this book.
thought to address it? The renowned philosopher, David Rodin, recently leveled the same objection regarding the use of just war reasoning (as I prefer to call it) in the case of humanitarian intervention, simply because military intervention for humanitarian reasons is not war, and treating it as if it were “deforms[s] key aspects of humanitarian intervention.”

Offering such characterizations presumes, however, that everyone understands and agrees upon what “just war theory,” or the “just war tradition,” itself is, and, in particular, that it is uniquely focused only on offering a procedure for deciding upon the moral justification for conventional use of force. This is analytically (circularly, or by definition) true, of course, since the tradition of specific discourse about the moral justification of war arose historically in response to the ongoing and seemingly endless practice of declaring and waging conventional wars. And, of course, in that limited historical sense, Rodin is correct to wonder whether it can now be fruitfully extrapolated to something that is not war – whether that “something” be humanitarian military intervention, or other forms of “irregular” warfare, or (in the present case) cyber conflict.

In the case of cyber conflict, I plan to develop and extend a line of argument first suggested by one of Professor Dipert’s critics, Colonel James Cook (U.S. Air Force Academy), who has on several occasions offered the view that it is merely the early encounters and relative unfamiliarity with conflict in this new domain that yields such pessimistic assessments of the continuing relevance of law or moral philosophy. These anxieties, he allows, tend to fade as our familiarity with the new technology or practice grows, and our competence and facility in drawing meaningful analogies with the known, tried, and true develops accordingly.

Cook’s very gracious and thoughtful assessment of this state of affairs thus agrees, at least on this one important point, with a far more strident account recently offered by Schmitt

---


himself, in a rather blunt “Foreword” written for a remarkably thoughtful and constructive new collection of essays on the problem of cyber war, edited by Jens David Ohlin, Kevin Govern, and Claire Finkelstein.\textsuperscript{36} In the opening pages of this important new work, Schmitt claims that, in effect, “all experts agree” that contemporary \textit{jus ad bellum} and \textit{in bello} (at least as these concepts of “justified resort to, and the proper conduct of, warfare,” respectively, are enshrined in international humanitarian law) can be made to apply without ambiguity or question to all these new dimensions of cyber conflict. This is so, he further argues, whether these take the form of war and military weapons, or “under the threshold” activities like espionage – and even further, that this fact has been acknowledged by all relevant subsidiary organs of the United Nations and the International Committee of the Red Cross, from whence this apparent consensus is “quite frankly, indisputable.”

This self-confident assurance of consensus is, however, less obvious in the other contributions to this important new anthology. One of the editors, Jens David Ohlin, opines in his own essay, for example, that cyber conflict and the so-called “problem of attribution,”\textsuperscript{37} as well as of intent, muddy the legal waters considerably. International law of armed conflict has, in particular, he objects, paid insufficient attention to a principle paramount in domestic criminal law: that of causation. Agents are held legally liable for those actions of which they themselves were the cause (with “intent,” and foreknowledge or premeditation, serving to determine the degree of liability and punishment likely accorded in response). International law needs to be specifically amended, in the aftermath of new problems generated by cyber conflict, to address this issue more explicitly.\textsuperscript{38} In similar fashion, Jim Cook, in his own essay for that same volume, concludes by allowing that, in important respects, “…cyber weapons [continue to remain] morally different from other tools of war.”\textsuperscript{39}

In somewhat more measured and moderate tones, Schmitt himself subsequently acknowledges standing problems of legal interpretation that remain in dispute, such as whether “interference with functionality” (as experienced during the DDoS attacks in Estonia) constitutes

\textsuperscript{36} \textit{Cyberwar: Law and Ethics for Virtual Conflicts}, loc. cit., pp. v-viii.
\textsuperscript{37} The “problem of attribution” is defined and briefly discussed in Singer and Friedman, pp. 59-63. We will return to this problem, and the extent to which it can be solved, later in the book.
\textsuperscript{38} In \textit{Cyberwar: Law and Ethics for Virtual Conflict}, see chapter 3, “Cyber Causation,” pp. 37-54.
\textsuperscript{39} \textit{Ibid.}, p. 36.
“damage” on par with physical damage or injury, and if so, how much interference is required to exceed that threshold. He likewise worries that the very exercise of applying international legal norms to the cyber domain will likely uncover lacunae in the law that need to be addressed (presumably along the lines that Ohlin and other contributors then proceed to propose). It appears, for the most part, that lawyers and philosophers are (or should be) allies and not enemies in this common endeavor, and that Schmitt’s evident exasperation in this foreword is mostly with moral philosophers or ethicists who carelessly and indiscriminately conflate moral with legal norms, and in so doing, he charges, “badly mangle the law.”

I find little cause to doubt Schmitt’s complaint, having been guilty on occasion of engaging in this “mangling” myself. Therefore let us resolve in the present project both to foregove this error, and to avoid inflaming these cross-disciplinary tensions any further. Conflation and confusion are perhaps inevitable in discussing a topic of such diversity and complexity as cyber conflict. And, to be fair, “lawyers do it, too!” Legal staff of the ICRC, for example, refer formulaically to the “five pillars” of international humanitarian law: “distinction, proportionality, and military necessity,” together with “command responsibility” and the prohibition of “superfluous injury and unnecessary suffering.” Yet, while it is convenient to summarize the content of international humanitarian law in this fashion, since all of these important legal norms are indeed embodied in various ways in specific legal statutes, none of those norms is itself a law. Rather, all are legal norms that inform the eventual codification of black-letter law. The explicit history and origin of those norms, in turn, lies in the moral discourse about war cited briefly above, and known as the “just war tradition” (which is why “mangling” and conflation frequently occur on all sides of this discussion).

---

40 Ibid., p. vii.
41 Indeed, many hold that this distinction upon which Schmitt insists simply cannot be categorically made, owing to the intertwining of moral and legal considerations. E.g., one of Europe’s leading arms control experts, Professor Harald Müller at Goethe University (Frankfurt) argues, in the case of the tension between other new norms (like the Responsibility to Protect) and the prevailing norm of “non-intervention,” that: “it would be wrong to see this as the collision between the legal and the moral [since] non-intervention is a norm meant to prevent war [and] this has a deep moral content, because war...inevitably has immoral consequences, even if fought for justifiable reasons. Thus, it is of little use to maintain a categorical distinction between legal and moral norms; rather we must think of all [state] behavior under the logic of appropriateness as unequivocally having a moral component, whether legally codified or not.” Norm Dynamics in Multilateral Arms Control: Interests, Conflicts, and Justice, eds. Harald Müller and Carmen Wunderlich (Athens, GA: University of Georgia Press, 2013): 5 [my emphases].
There is perhaps too much remaining to be done in the cyber realm to be de-railed by such petty disciplinary squabbles, although Schmitt’s implicit demand for rigor and clarity, as well as caution and care in respecting important distinctions, remain well-advised.

The origins of international law pertaining to war and armed conflict within the older and broader moral discourse about war in the Western world is fairly well established, and reasonably well understood.\(^{42}\) So, for that matter, are the historical origins and basic contents of JWT itself. What is decidedly less well understood is the underlying nature of just war reasoning: not where it arises (although it in fact transpires in far more multicultural contexts than are usually attributed to it), but what it is, and what gives it jurisdictional authority, or what I termed above, “normative force.” Why, that is to say, should anyone – and especially those nations and peoples outside the traditional boundaries portrayed in the history of JWT – pay any attention to its principles or constraints on declaring and waging war (whether conventional war or cyber war)?

There have been many recent important attempts to engage in the “revision” of just war theory by challenging some of its most fundamental and cherished concepts, such as "proportionality" (in both the decision to resort to war, and the subsequent waging of it); whether national self-defense constitutes a sufficient "just cause" for war; and especially whether a norm or principle known as "the moral equality of soldiers" deserves to be enshrined (as it presently is) in the law of armed conflict.\(^{43}\) Surprisingly, however, the underlying question about JWT’s very nature and source of normative authority remain altogether unaddressed. JWT continues for the large part to be portrayed merely in historical and cultural terms, as an artifact mainly of the

\(^{42}\) The references for this history are too numerous to cite here, but are cited at length in a summary discussion of that history and reciprocal relationship in Chapter Two, “Ethics and International Law,” in my recent book, Military Ethics: What Everyone Needs to Know (New York: Oxford University Press, 2015).

\(^{43}\) The pioneering work of David Rodin, War and Self Defense (Oxford 2002) and of Jeff McMahan, Killing in War (Oxford 2009) occupy center stage in this important discussion, to which numerous thoughtful critics and scholars have made substantive additional contributions as so-called “revisionists.” Many also credit Thomas Hurka’s widely-cited "Proportionality in the Morality of War," Philosophy and Public Affairs 33, no. 1 (2005): 34-66 with having helped to launch the revisionist JWT movement. Yet for all its lengthy and disjointed rambling, this poorly-edited and thinly-argued article fails even to note the use of proportionality routinely in numerous similar contexts of moral discourse involving making a justified exception to prevailing norms and moral principles (see below). Other important figures and works in this movement include: Cecile Fabre, Cosmopolitan War (Oxford: Oxford University Press, 2012); Cecile Fabre and Seth Lazar, eds. The Morality of Defensive War (Oxford: Oxford University Press, 2014); David Rodin and Henry Shue, eds., Just and Unjust Warriors: The Moral and Legal Status of Soldiers (Oxford: Oxford University Press, 2008). This is only a small sample of the extensive literature on this topic.
Christian West, with little or no authority or obvious applicability to cultures and civilizations in other historical eras, or in other parts of the world today.

At the same time, JWT is the origin (as mentioned above) of all of the legal norms that now infuse and inform international law, which itself lays claim to universal jurisdiction. Hence, either we must conclude that this entire body of international law is grounded in nothing more than cultural bias (which constituted the Chinese and Russian objections to the Tallinn Manual, in particular); or else we must demonstrate that the moral and legal norms that underlie it have a much broader purchase than their history, and even the respect accorded some of their most venerable figures (such as Hugo Grotius, Emer de Vattel, Francisco Vitoria and St. Thomas Aquinas), can explain.

I thus propose to probe behind the squabbling between law and morality regarding jurisdiction over cyber conflict, and to make a case instead for the importance of the moral and legal norms that both disciplines seek to preserve and recommend within the new domain of cyber conflict. In order to accomplish this, however, it will prove necessary to address this profound, underlying lacuna in the underlying nature and authority of JWT itself.

Accordingly, in this work, I put forward a new “theory of Just War Theory” (as well as of international law) – one that grounds both the law of armed conflict and JWT (encompassing in each case both jus ad bellum and jus in bello) in a more fundamental kind of moral discourse – a genus of which both are distinct species.

It is difficult to know quite what label to affix to this discourse: it could well be called “the morality of exceptions,” or “the ethics of exigencies,” or even (in a sense quite different than originally intended by J.L. Austin44), “a plea for excuses” or a “request for exemption.” In particular, I will demonstrate that such reasoning, and the list of necessary conditions for granting the excuse or exemption (or for acknowledging the exception or exigency at hand), is found in many other species of moral and legal discourse as well: that concerning civil

44 J.L. Austin, “A Plea for Excuses,” Proceedings of the Aristotelian Society 57 (1956): 1-30. This famous article merely sought to call attention to important distinctions encapsulated in ordinary language, e.g., between “mistakes” and “accidents” that might attend a request for being excused from blame for one’s actions. This, unfortunately, is typical of the thin gruel that constituted (analytic) “philosophy” during this epoch, and I clearly have something a bit more significant in mind.
disobedience, for example, and killing (when undertaken in self-defense or in the defense of others from attack). Its structure is discerned in the family resemblances between those resulting lists of necessary conditions, as encountered ubiquitously in moral discussions about when lying, or the forfeiture of contracts, or the breaking of solemn promises, or the forsaking of individual or group loyalties – all things that more or less everyone, everywhere, and at all times deem *prima facie* impermissible – are nonetheless found in extreme circumstances to be at least permissible, if not morally obligatory. Indeed, a hint of how this all works in general is also found in the controversial and contested just war discussion of “supreme emergency.”

In all such instances of moral reasoning, and in all such species of this genus of moral and legal discourse, I will argue that one finds demands for an overriding reason or “just cause,” alongside some form of requirement for “peer review” or “publicity” as finally constituting the sole form of "legitimate authority" to grant the exemption. One invariably finds as well the demand that any such exemption from strict adherence to the prevailing norms of conduct in these distinct realms be granted (or acted upon) only as a last resort. One also finds, in such species of moral discourse, requirements or constraints on how the exemption can be exercised when approved: for example, with respect to the harm that will thereby be done in comparison with the good or goal to be accomplished (“proportionality”), which is frequently coupled with a demand to limit any resultant harm to morally relevant agents (“discrimination” or “distinction”). Agents empowered to exercise a grave exemption from prevailing norms are also required to insure that this "collateral damage" will be deemed permissible only in pursuit of tactical objectives which promise to be absolutely essential to accomplishing the original justified strategic goal (“necessity” in furtherance of the “just cause”). Such forms of moral and legal

---

45 The concept of a “supreme emergency” during wartime constituting a case for exemption from its normal moral and legal constraints was first raised by Michael Walzer as a possible justification for Winston Churchill’s decision to deliberately violate the laws of armed conflict by bombing civilian targets during WW II. See *Just and Unjust Wars* (New York: Basic Books, 1977): Chapter 16. It has been much critiqued since (e.g., Martin L. Cook, “Michael Walzer’s Concept of Supreme Emergency,” *Journal of Military Ethics* 6, no. 2 (2007): 138-151), but Stephen Coleman at the Australian Defence Force Academy was the first to recognize that the pattern of justification utilized for supreme emergencies mirrored that of just war theory itself during a presentation on “supreme emergency” at the third annual conference of the European Society for Military Ethics (Shrivenham.: U.K. Defence Academy Command & Staff College, 2013).

46 Public questions about the quality and appropriately-adversarial stance of this “peer review” of clandestine activities came to occupy center stage in the ensuing debate about Snowden and the NSA’s programs, for example.
reasoning are, accordingly, hardly limited to war and its conduct – although these are among the most important of the cases that elicit such reasoning.

Finally, to explore the significance of this feature of moral discourse for cyber warfare, we will be led in this book to explore its impact on the emergence and formation of appropriate norms of moral and legal conduct. This is a crucial and, indeed, hopeful development in the cyber domain, as information technology expert Pano Yannakogeorgos at the U.S. Air Force Research Institute (Maxwell AFB, AL) has pointed out.\(^47\) The concept of “emergent norms” is well-established in the fields of political science and international relations.\(^48\) But such a concept is viewed with deep suspicion and skepticism in moral philosophy, where norms as moral principles are thought to be utterly distinct from practice (otherwise, how could they legitimately be said to “govern” practice?). Indeed, to attempt to drive norms (“best practices,” or ideals concerning how individuals and nations ought to behave) from descriptions of current practices (i.e., deriving “ought” from “is”) is thought to constitute a fundamental logical fallacy, often labeled “the naturalistic fallacy.”\(^49\)

\(^48\) See Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” International Organization 52, no. 4 (Autumn 1998): 887-917; Richard Price, “Moral Limit and Possibility in World Politics,” International Organization 62, no. 2 (April 2008): 191-220; and the essays collected in Implementation in World Politics: How International Norms Change Practice, eds. Alexander Betts and Phillip Orchard (Oxford: Oxford University Press, 2014). See also Müller and Wunderlich (n. 30, above). This important literature from political science and international relations, however, is primarily oriented toward offering (against realists and functional realist critics) an empirical account of how “ideational” (moral) norms affect state policy and political change. My own efforts in this book are accordingly directed toward providing a conceptual foundation for the historical and descriptive accounts of “norm dynamics” offered by social scientists. In particular, I seek to demonstrate how norms “emerge” and why, as a result, they are able to manifest the universal normative behavioral influence on state behavior empirically attributed to them by these other scholars.
\(^49\) The original formation stems from the work of Scottish Enlightenment philosopher, David Hume, in his Treatise on Human Nature (section 3.1.1, “Moral Distinctions not derived from Reason”), in which this formidable skeptic complains of the prevalence of a widespread but unexplained transition in “vulgar systems of moral philosophy” between discussions of “what is or is not” a matter of fact or reason, to what “ought or ought not” to be permitted as a condition of morality. Whether or not this is taken as a legitimate formal logical fallacy (it is often found in standard logic texts classified merely as an “informal fallacy”), it was finally redressed in the work of Richard M. Hare in 1952, who defined carefully the formal conditions under which an obligation (“ought”) could be derived from statements of fact (“what is or is not”), when the specific obligation was derived from a “practical syllogism” whose major premise was some broadly-recognized principle guiding or constraining conduct in the general case: see The Language of Morals (Oxford: Clarendon Press, 1952). The origins of this fallacy are often erroneously attributed, however, to G.E. Moore, who formulated a quite distinct version of a “naturalistic fallacy,” not addressed to Hume’s original problem of the relations between descriptive facts and moral obligations, but instead.
How then, we must ask, can norms of practice legitimately “emerge” from practices themselves? And what prospect does this larger conception in international relations and state behavior hold for cyber conflict?

Clearly, in an important sense, “norms” as a fundamental feature of both law and morality, particularly in regard to state behavior, are “under-conceptualized.” That is (exactly as will prove the case with the lacuna detected in JWT above) despite numerous accounts of how norms function in interstate conflict, and which norms are currently recognized and respected, it remains something of a mystery of where they come from, and particularly of how they can blandly be described as “arising or emerging” from practice, apart from peculiar accidents of history and custom. And history and custom, by themselves, are utterly lacking in normative force. Hence, I will be obliged in this book to demonstrate that norms of behavior governing new or novel situations always arise from reflection (from the standpoint of the aforementioned considerations of just cause, last resort, proportionality and the like) on better and worse reasons for engaging in otherwise-proscribed behaviour, as well as (in afterthought) on better and worse forms of subsequent conduct when doing so.

This is a particularly formidable problem to tackle, and will require at least passing reference to important contributions made in this area by political and legal philosophers like Jurgen Habermas and John Rawls, as well as Immanuel Kant (upon whose treatment of the duties of justice and of virtue in his later Metaphysics of Ethics (1795) both based their own respective treatment of these problems of moral reasoning and the universal authority of resulting norms and principles). Surprisingly, the discussion also leans heavily on the thought of Aristotle and Alasdair MacIntyre, the latter of whom is usually taken to be a harsh critic of abstract and de-contextualized moral reasoning after the fashion of Kant. But it will prove to be MacIntyre’s account of how moral norms arise from practice, and from ensuing reflections upon practice, that in turn informs what sorts of norms are worthy of universal jurisdiction (the problem addressed by Habermas and Rawls, but found much earlier in the initial methodology of Aristotle’s seminal works on ethics and politics). In particular, MacIntyre’s account of Aristotle denying that the Good was a natural kind, or could itself be derived from purely naturalistic considerations, as utilitarians from Bentham to Sedgwick had routinely attempted to do. Moore’s version, originating in his doctoral dissertation on Plato, stemmed from his unwavering conviction that “the Good” (whether in morals or aesthetics) was itself a primordial and indefinable conception from which all else derived.
will be found to provide the conceptual framework that clarifies how governing principles, which are finally orthogonal to practice, can and do nonetheless arise from, and within the midst of, practice. This occurs through a peculiar kind of reflection on practice, a kind of “reflective equilibrium” that differs from that described by Rawls in particular. Instead, as MacIntyre demonstrated more than two decades ago, this original “reflective equilibrium” is simply “practical reasoning” (phronesis, particularly as guided by the kind of experienced and rationally-informed judgment that arises from the possession of sophrosyne), of the sort exemplified by Aristotle in his important works on moral and political philosophy (as well as on the physical and biological sciences), and subsequently described by him as the methodology appropriate for these “imperfect” or “incomplete sciences” in his great work of logical method, the Posterior Analytics.

That Kant and Aristotle, the most important ancient and modern figures for the understanding of both morality and law (alongside contemporary exemplars, such as Rawls, Habermas, and MacIntyre, respectively) should figure large in the background of my discussion should not be gainsaid. But the present work is devoted specifically to bringing order out of the chaos that is conflict in the cyber domain, and is intended for a wider audience than scholars merely of moral philosophy or jurisprudence. Hence, while acknowledging and invoking these sources in the course of this work, I will do my best to avoid bogging down the majority of readers in technical discussions which would likely prove all but unintelligible, let alone of any interest, to more than a very few.

The important fact to bear in mind is that only through such an examination (however cursory or incomplete) of the sources of moral and legal authority and jurisdiction can we answer the questions at the forefront of our inquiry, concerning both what laws and moral principles should be properly invoked in the cyber domain, as well as (even more importantly) why these might finally be said to hold sway, wield authority, or have any resulting “normative force” in that domain – or, for that matter, in any domain in which they are currently applied.

This rather tedious slogging will be necessary to return us, in conclusion, to a consideration of normally prohibited activities such as lying, deception, disloyalty, the breaking or voiding of contracts and violating of oaths.
For Edward Snowden unquestionably did all of these things, when violating law and agency regulations, stealing highly classified data, and bringing this to the attention of the wider public (including America’s staunchest adversaries in cyber conflict). His justification for doing so was that he was said to have been engaged in “whistle-blowing.”

“Whistle-blowing” is a form of civil disobedience in an organizational setting that generally involves violating laws and regulations to which one has previously given assent (through the voluntary swearing oaths, the making of promises, and the signing of contracts). More than anything else, “whistle-blowing” constitutes the height of disloyalty to one’s own immediate group. This is why it is so dangerous, so poorly received and imperfectly understood by the immediate victimized group, and more widely thought to be among the forms of exceptional activity (like war itself) for which the “reasoning about exceptions” is most urgently required. To “blow the whistle” on your organization’s activities inaccurately is similar to going to war unjustly, in error. It is a serious mistake, with damaging consequences, for which one is morally culpable.

The whistle-blower, like the civil disobedient, therefore must willingly take upon himself the responsibility for engaging in this activity, including the moral opprobrium with which the organization and wider public are likely to respond (until they have had a full opportunity for “peer review” and evaluation). Importantly, he must undertake this activity only as a last resort, when lesser measures have been tried. The harm done by the whistle-blowing itself must, moreover, prove to be proportionately less than the good achieved (or else, proportionately less than the degree of wrong-doing and harm by the organization thereby exposed).

Using an analogy drawn from Wittgenstein (but beholden to Kant), I will argue that this is always a “public,” and never meaningfully a “private” act. In my concluding chapter, I will argue that Snowden, finally, fulfilled none of these requirements. He imposed and acted on his own, entirely private, facile, and wholly unvetted notions of personal privacy, and on what he took to be its manifold violations by the NSA, without due deliberation or any discernible form of wider public discussion, even if he sincerely believed in his “just cause.” And if (as Wittgenstein claimed) there can be no meaningful “private language” with which to describe one’s pain, it is even more the case that there can be no private language in which to describe one’s justified cause. Both are inherently public phenomena.
Snowden’s own privately-premeditated actions, moreover, were those of a comparatively young and poorly-oriented newcomer. They were decidedly not the result of sober judgments, reluctantly reached by a seasoned, experienced and thoughtfully reflective organizational veteran (like Daniel Ellsberg, decades earlier, had proven to be within the Department of Defense under similar circumstances). Having failed to comprehend, let alone fulfill the responsibilities incumbent upon the whistle-blower, Snowden unsurprisingly erred in equating a well-intentioned (if paternalistic) program of national self-defense in which he and his organization turned out to be deeply engaged, with a much different, highly malevolent program of unauthorized and unsupervised surveillance (which he and others equated with the practices of the East German Stasi). In so doing, in error, he did and continues to do irreparable harm to this nation’s security.

His (unjustified) actions did finally serve a larger purpose, however, in framing the question with which we ourselves must conclude. The Snowden affair proves relevant to this book on ethics and cyber warfare, that is to say, because it lies at the heart of considerations rightly laid before the public, regarding the price they are willing to pay in terms of their privacy and liberty for the sake of security and national self-defense against aggression.

What level of insecurity is the public willing to shoulder, in particular, in order to maintain, not simply their own personal privacy, but also the continuing anonymity of actors in the cyber realm -- anonymity that currently allows malevolent cyber actors to do whatever they please without accountability? This concluding question is a question at least as old as that posed by Thomas Hobbes, who forcefully argued that in an imperfect world, individuals must be willing surrender a measure of these natural rights for the sake of peace, order, security and the rule of law (even assuming that “anonymity” should be numbered among those rights). Such a political compromise has thus far, however, seemed beyond reach in the cyber domain….at least, for the time being.