FOREWORD
Cyber Warfare, What are the Rules?
By Daniel B. Garrie

ARTICLES
Cyber Attacks and the Laws of War
By Michael Gervais

If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare.
By Michael Preciado

They Did it For the Lulz: Future Policy Considerations in the Wake of Lulz Security and Other Hacker Groups’ Attacks on Stored Private Customer Data
By Jesse Noa

A New Perspective on the Achievement of Psychological Effects from Cyber Warfare Payloads: The Analogy of Parasitic Manipulation of Host Behavior
By Dr. Mils Hills

Volume 1 | Winter 2012 | Issue 1

www.jlcw.org
EDITORS
Daniel B. Garrie, Esq., Editor-in-Chief
Siddartha Rao, Esq. Executive Editor

Associate Editors
Candice Lang, Esq., Editorial Fellow
Stephen Williams, Esq., Editor-at-Large

EDITORIAL BOARD
William Spernow
Alex Carrillo
Uma Chandrashekhar
Patrick Grey
Thomas A. Johnson
Jonathan E. Turner
Judge David Harvey
Michael Schmitt

Jeff Bardin
Dick Crowell
Gus Dimitrellos
George Hull
Alan Roper
Russell Walker
Joseph E. Weiss
Larry Ponemon
Cyber Warfare, What Are The Rules?

By Daniel B. Garrie*

What is not cyber-warfare? Al-Qaeda terrorists fly two jetliners into the twin towers killing almost 3,000 people.¹ An American plane flies over Hiroshima and drops an atomic bomb killing over 90,000 people.² The Nazis force hundreds of thousands of people into gas chambers and kill millions of people.³ A group of soldiers execute hundreds of innocent people.⁴ A

* Daniel Garrie is the Senior Managing Partner and co-founder of Law & Forensics LLC a boutique consulting firm specializing in complex e-discovery management, digital forensic investigation, and cyber security preparedness. Mr. Garrie has served as an Electronically Stored Information Liaison, Forensic Neutral and Expert for the L.A. Superior Courts, 2nd Circuit, 3rd Circuit, 7th Circuit, New York Supreme Court, and Delaware Supreme Court. He has published over 100 articles, been cited by the Supreme Court, and the second edition of his treatise Dispute Resolution and E-Discovery will be published by Thomas-West in 2013. He can be reached at Daniel@lawandforensics.com


military releases poisonous gases upon opposing forces.\textsuperscript{5} All of these actions if committed constitute acts of war and war crimes (albeit some may argue that not all of these acts constitute war crimes).\textsuperscript{6} While the devil is in the details, the crux is that in all of these scenarios there is physical evidence: DNA, radiation signature, witnesses; bullets; and gas residue.\textsuperscript{7} In cyber warfare, what is the physical evidence? A binary string of 10101010 in the digital ether?

Since the establishment of the United Nations, wars of aggression have been outlawed,\textsuperscript{8} and multilateral conventions refer to “armed conflict” instead of “war.”\textsuperscript{9} The word cyber does not appear in these texts or in the


\textsuperscript{9} “The law of war is to be found not only in treaties, but in the customs and practices of states which gradually obtained universal recognition, and from the general principles of justice applied by jurists and practiced by military courts. This law is not static, but by continual adaptation follows the needs of a changing world.” \textit{Trial of the Major War Criminals Before the International Military Tribunal, Nuremberg}, 14 November 1945–1 October 1946 (Nuremberg, Ger., 1947), 221.
multitude of others that adjoin these legal frameworks.\textsuperscript{10} This Journal seeks to promote legal scholarship that can aid the global community as a whole to address this new dimension of war. With the advent of cyber warfare the complexity of what is war is even more clouded and the application of law to this is even murkier.

The focus of this journal is on cyber-warfare.\textsuperscript{11} Cyber-warfare occurs when one country perpetrates a cyber attack against another country that would to the reasonable person constitute a state act of war.\textsuperscript{12} The purpose of the Journal is to encourage dialog to explore and define what constitutes a cyber attack and what constitutes a reasonable expectation of cyber-security.\textsuperscript{13}

Below are two of the hundreds of scenarios on which the law remains silent: Would a cyber-assassination by a foreign government constitute an act of war? Is a nation’s cyber attack initiated in self-defense

\textsuperscript{10} Vida M. Antolin-Jenkins, \textit{Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?}, 51 \textit{NAVAL L. REV.} 132, 140 (2005); Frank J. Cilluffo et al., \textit{Bad guys and good stuff: When and where will the cyber threats converge}, 12 \textit{DEPAUL BUS. L.J.} 131 (1999).


\textsuperscript{12} Stephen Dycus, \textit{Congress’s Role in Cyber Warfare}, \textit{J. NAT’L SECURITY L. & POL’Y} 155, 162 (2010) (“Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both.”); Understanding Cyber Warfare, \textit{available at} \url{http://cyber.laws.com/cyber-warfare} (last visited Feb. 5, 2013).

that results in the deaths of thousands of civilians an act of war? Is it a war crime?

The assassination by bullet of a foreign leader is an act of war and proving it is a matter of using the physical evidence to connect the dots.\(^\text{14}\) However, what about an individual working for a foreign government attends a speech, say at the United Nations, and using a wireless device kills five world leaders by sending a signal to their pace makers or insulin pump, that tells the device to send a fatal dose.\(^\text{15}\)

In this scenario, a trail will be hard to find and even if found, it could be a plant, meaning spyware could have been used to put spyware on an unknowing attendee who by simply turning their phone to silent triggered the incident.\(^\text{16}\) This scenario, where five foreign leaders may have been assassinated by a foreign government, raises a slew of complex and new legal issues, such as: How do we prove a country was an actor? What evidence is needed to establish guilt? How does one acquire such digital evidence?

Another complex scenario, a foreign government defends itself (pre-emptively or post cyber attack) against a cyber attack and in defending itself retaliates in a way that results in massive civilian


\(^{16}\) Major Erik M. Mudrinich, Cyber 3.0: The Department of Defense Strategy for Operating Cyberspace and the Attribution Problem, 68 AFL REV. 167 (2012).
deaths. For example, say a foreign government is cyber attacked by several foreign governments that results in a nuclear powered aircraft carrier almost melting down, which if it had melted down would have killed thousands of civilians. As a defensive measure the attacked country responds triggering defensive digital counter cyber attack that results in the foreign governments’ power grids going down, causing tens of thousands of civilian deaths. The origin of the power failure was the counter attack, but the fragile infrastructure, feeble cyber security, and the antiquated state of the power grid all contributed.

The aforesaid defensive scenario presents a slew of issues, including: whether a non–lethal cyber warfare attack is a “use of force” that can be returned, or merely an act that violates international law.

Would the defensive counter measures constitute an act of war? Do they constitute war crimes against humanity? Who is to be held responsible? The computer programmers who wrote the code? The military project manager who oversaw the creation of the code? The commander who hit the button setting off the event? The hardware engineer who created the computers that enabled the attack? What constitutes an act of war is blurred? Moreover, establishing who is the perpetrator, or enemy, in a cyber warfare scenario is an even greater challenge.

As a cyber-security and legal professional where I am asked to bridge these realms I often find that many

---


scenarios lack bright lines as in the examples above, which makes the legal realm even more complex.

As a bridge between these realms, it is apparent there is a vast divide between the cyber and legal realms. No one disputes that (1) the digital realm blurs the complicated and often confusing rules that govern modern day warfare and (2) the rules of warfare have changed and will continue to evolve. It is my belief that the threshold is shifting and thus mandates the need to redefine the act of war itself and the laws that govern the conflict.19 The focus of the Journal of Cyber Warfare is to ask these tough questions and engage legal,

19 As a response to cyber intrusions by foreign groups against US commercial interests, the President should consider an executive order expanding the powers of the Federal Intelligence Surveillance Court (or FISC) to allow companies to petition for a government response to offenses committed against the company. Presently in the United States, the FISC is responsible for issuing warrants for domestic surveillance of suspected foreign operatives in the U.S. Between international arbitration, FISC, and civil courts; corporations that are hacked by agents of sovereign nations have little realistic recourse.

Imagine a scenario whereby an American corporation in the aerospace industry is hacked. All investigations point to the responsible party being an agent of a sovereign nation. While the corporation may be able to recover fiscally through insurance policies, the damage to the industry and the ability of this company to compete nationally and internationally is permanently altered. With an expansion of the FISC, this corporation would be able to petition a government body, such as the Department of Defense. If the DOD agrees with the seriousness of the hack and the long standing implications of this act, then the DOD would then make a special appeal for emergency action on behalf of the company that would be heard within 24 hours. If the expanded FISC agreed that action was necessary, the DOD would be permitted to take action against the sovereign nation.

This expansion of the court would require an expansion of the bench, a position which I would openly pursue to ensure the judiciary is fully informed on the ways and means of cyber intrusions.
technology, government, and to shape the evolution of these new rules of war.
Cyber Attacks and the Laws of War*

By Michael Gervais**

I. INTRODUCTION

In 1949, John Von Neumann—a mathematician and an early architect of computing systems—presented at the University of Illinois a series of lectures called the Theory and Organization of Complicated Automata, where he explored the possibility of developing machines that self-replicate.¹ Von Neumann envisioned machines that could build self-copies and pass on their programming to their progeny. While his ideas had legitimate applications, such as large-scale mining, many observers also consider it to be the theoretical precursor to the modern-day computer virus.² Self-replication is a defining characteristic of computer viruses and worms. Through self-replication, computer code populates computer systems exponentially. Computer viruses and worms have the capacity for constructive applications,

* A version of this article appeared in the Berkeley Journal of International Law. Michael Gervais, Cyber Attacks and the Laws of War, 30 Berkeley J. Int’l L. 525 (2012). It has been modified and reprinted here with the express permission of the Berkeley Journal of International Law.

** Michael Gervais graduated in 2011 from Yale Law School, where he served as senior editor of the Yale Journal of International Law (YJIL). Before law school, Michael Gervais spent time serving as an AmeriCorps* VISTA and as a Jesse M. Unruh Assembly Fellow in the California State Legislature.

² Id.
but they are most often malware—malicious software that is hostile, intrusive, and unwelcome.\(^3\)

The first generation of malware in the 1970s was mostly experimental and did little damage beyond using computer memory and annoying its victims. When personal computing took hold in the 1980s, malware evolved into something more destructive. Viruses, worms, and other forms of malware spread quickly throughout the Internet, destroying data, overloading systems, and generally causing havoc.\(^4\) The Advanced Research Projects Agency (ARPA)—a research wing of the US Department of Defense (now known as DARPA)\(^5\)—responded by funding a Computer Emergency Response Team at Carnegie Mellon University to coordinate and respond to computer security issues.\(^6\) Additionally, ARPA asked the National Research Council (NRC) to study the “security and trustworthiness” of American computing and communications systems. In 1991, the NRC issued its report. Presciently, the report noted that “[t]omorrow’s


\(^5\) DARPA and ARPA are used interchangeably because the agency recently switched its name from the Advanced Research Projects Agency (ARPA) to the Defense Advanced Research Projects Agency (DARPA).

terrorist may be able to do more damage with a keyboard than with a bomb.”

It has been over twenty years since the NRC highlighted the risks to computer systems. Since then, the global community has grown more reliant upon the everyday use of computers and the Internet. The ever-increasing interdependence of computer networks has sparked a parallel growth in the complexity of cyber attacks. As computer systems have evolved, so have the attacks. Infrastructure, the financial system, commerce, government operations, including the military and, ultimately, national security have gone online, leaving the “security and trustworthiness” of the computing and communications system’s increasingly vulnerable to hostile actors. With each new cyber attack, nation-states are seeing the potential vulnerabilities—as well as opportunities—of an interconnected society. Cyberspace has become a new battleground for warfare.

The lawfulness of cyber warfare remains unsettled. The international community designed the international instruments that form the laws of war in response to kinetic technologies. As warfare evolves with new technologies, our understanding of how to interpret these international instruments changes as well, leaving decision makers uncertain as to how to apply the laws of war to cyber attacks. This is a troubling scenario because recent events confirm that cyber warfare is operational. Although still in its infancy, the capabilities of cyber attacks are innumerable. This article examines the capabilities of a cyber attack and the relationship between cyber attacks and the existing international instruments that govern the laws of war.

---

Part I discusses the architecture of cyberspace and how it operates. Part II examines the framework of international humanitarian law and its application to cyber warfare. Ultimately, I contend, the international instruments in place do not answer all the relevant questions that cyber attacks generate. Indeed, they cannot even answer all the questions surrounding the forms of warfare that they were created to govern. However, these international instruments are helpful in determining how cyber attacks ought to be understood under the existing *jus ad bellum* (use of war) and *jus in bello* (wartime conduct) frameworks.

A. SHORT HISTORY OF CYBERSPACE AND ITS ARCHITECTURE

The Internet is a by-product of the science and technology race of the Cold War. After World War II, tension quickly escalated between the United States and the Soviet Union. The Soviet Union’s launch of the Sputnik satellite in 1957 caused particular alarm in the United States.9 The launch changed world perception of the United States as a technological superpower, creating a sense of vulnerability among the American people, and elevating the international status of the Soviet Union.

With the threat of nuclear war looming over the nation, the US government responded to the perceived gap with a shift in strategy that emphasized technology and science.10 The federal government poured money into science, engineering, mathematics education and research at all levels. Among its many initiatives, the

---


United States created and funded the Advanced Research Projects Agency (ARPA) within the Department of Defense a few months after the launch of Sputnik. Its task was to maintain the technological superiority of the US military and prevent “technological surprise.” It would prove invaluable for the creation of the Internet.¹¹

One concern for the military was the theoretical ability of a Soviet nuclear strike to disable completely American communications systems. The prevailing view was that the command and control structure of the US government and military could not withstand such an attack. Therefore, military analysts saw a robust communications network that would survive an attack as a necessity in any nuclear confrontation.¹²

The critical component of survivability was a technique called “distributed communications.” Under conventional communication systems, such as telephone networks, switching, i.e., the process of channeling data from input to output ports, was concentrated and hierarchical.¹³ Thus, a call went to a local office, then to a regional or national switching office if a user needed a connection beyond the local area.¹⁴ Under this system, if a local office were destroyed, many users would be cut off. Responding to this communications threat, Paul Baran, a researcher at the Air Force’s think tank, the Rand Corporation, conceived of a distributed system composed of multiple switching nodes with many attached links.¹⁵ Under Baran’s system, if one node failed, the information would simply take an alternative route. This redundancy made cutting off service to users

¹⁴ *Id.*
¹⁵ *Id.*
more difficult. Moreover, Baran proposed locating the nodes far from population centers to make the system more secure.

Most importantly, Baran created a technique of switching to move data through the network as packets—a series of binary numbers (“bits”). This innovation proved vital for several reasons: (1) fixed-size packets simplified the design of switching nodes, (2) breaking messages into bits of information made it harder for spies to eavesdrop on communications, and (3) the system was more efficient and flexible for sharing a data link. Although packet switching was inherently more complex because packets of information had to be reassembled for the user, researchers made the system for data transmission less costly to build. Reducing the costs of the system made it more feasible to create a highly redundant and therefore survivable communications system.

Meanwhile, ARPA hired J.C.R. Licklider to head the Information Processing Techniques Office (IPTO). Before joining IPTO, Licklider had imagined a nationwide network of “thinking centers,” with responsive, real-time computers. This vision underlay the ARPANET—the precursor to the Internet. As head of the IPTO, Licklider funded technology that put his ideas into practice. In addition, he warned that the dozen or so independent projects would produce incompatible

16 Id.
17 Id.
18 Id. at 17–18.
19 Id. at 19.
20 Id. at 20.
21 Id.
23 Id. at 79.
machines, incompatible computer languages, and incompatible software. However, it was not until the third IPTO director—Robert Taylor—that IPTO organized the fledgling projects around the country around a common vision. Rather than ARPA funding dozens of independent projects, Taylor decided that it was necessary for the remote projects to share computing resources. It was time to build a “network of networks.”

To create the ARPA network, researchers made several critical technical decisions that defined its architecture and that of its successor, the Internet. These decisions have ongoing implications for cyber attacks.

First, because there was insufficient funding for ARPA to build its own wires across the country, the government had to move its data through the civilian infrastructure already in place—the AT&T telephone system. Second, the government utilized Baran’s packet-switching concept. Thus, digital messages were broken into segments of fixed lengths rather than sent through the network continuously. This feature protected against static and distortion by isolating errors and giving the system a chance to fix them. Third, the ARPA network was decentralized. Adhering to Baran’s concept of a survivable communications system, rather than engage a master computer to sort and route the packets, each ARPA site read the digital address on the packet as it came in. The site then accepted the packet if the address was local or sent it in the right direction. Finally, instead of asking each site to run packets

---

24 Id. at 79–80.
26 Waldrop, supra note 22, at 80.
27 Id.
28 Id. at 81.
29 Id.
through its main computers, researchers built Interface Message Processors (IMPs)—the precursor to the modern router—that handled all the routing chores.\textsuperscript{30} By using IMPs to handle routing, the main computers on the network had to learn only the IMP’s language rather than the language of each computer on the network.\textsuperscript{31}

The next challenge was figuring out how to make all of the computers to work together. Because ARPANET linked together many one-of-a-kind machines,\textsuperscript{32} it was necessary for the various computers to adopt a standard universal protocol.\textsuperscript{33} By 1974, Robert Kahn and Vinton Cerf designed the standard protocol that is still in place today—the Transmission Control Protocol/Internet Protocol (TCP/IP).\textsuperscript{34} TCP/IP specifies how data should be formatted, addressed, transmitted, routed, and received at the destination. Over the next few years, Kahn and Cerf developed several operational versions of the protocol and, by 1982, the TCP/IP was reliable enough for the Department of Defense to make it the standard for military computer networking.\textsuperscript{35} Finally, in 1983, ARPANET switched over to TCP/IP—and the Internet was born.\textsuperscript{36}

Each of these decisions was critical to the formation of the modern-day Internet, but they also created a greater number of targets for cyber attacks. Furthermore, the decision to intertwine the civilian and military infrastructure made it difficult to determine which targets are valid under the law of armed conflict. Despite such consequences, these decisions clearly facilitated communication between computers.

\textsuperscript{30} Id.
\textsuperscript{31} Id. at 84.
\textsuperscript{32} ABBATE, \textit{supra} note 13, at 48.
\textsuperscript{33} See Waldrop, \textit{supra} note 22, at 84.
\textsuperscript{34} Id. at 85.
\textsuperscript{35} Id.
\textsuperscript{36} Id.
Once the fundamental architecture was in place, the private sector and researchers across the nation collaborated and improved upon others’ ideas to build applications that popularized the Internet for mass consumption. These applications included E-mail, the World Wide Web,\textsuperscript{37} file transferring, and a host of other programs connecting users to what is known as “cyberspace.”\textsuperscript{38} Moreover, with the advent of personal computers and Internet Service Providers (ISPs), which linked users to the Internet through the public domain, other networks began to connect to one another, which eventually made ARPANET obsolete.\textsuperscript{39}

Thus, over a period of thirty years, the initial problem of how to design a survivable system of communication yielded a tool that forever changed how people communicate. But the growing integration of computers into individuals’ lives also made the vulnerabilities of cyberspace increasingly apparent. The entire Internet is shared between civilian and military uses, and between the United States and its adversaries. This level of interconnectedness may be the Internet’s greatest virtue—expanding the number of users and creating a global marketplace of ideas—but it also presents a grave security risk.

The largest threats in cyberspace are not accidental. Rather, bad actors design malware to access a computer system without the owner’s informed consent. Malware—similar to software—consists of programs or protocols that tell computers what to do. Those instructions are often destructive, intrusive, or annoying.

\textsuperscript{37} Tim Berners-Lee, a computer programmer at CERN, developed the World Wide Web as a simpler way to provide access to research materials.


\textsuperscript{39} Waldrop, supra note 22, at 85.
Unfortunately, just as software has become more innovative and sophisticated over time, so, too, has malware. What began with initial users testing a computer system’s capabilities by exploiting its vulnerabilities has escalated into the use of malware to commit cyber crimes. As personal computing and the Internet have grown, the number and impact of bad actors has dramatically increased.

The first versions of malware appeared on the ARPANET as experimental self-replicating programs. Designed to annoy or harass users, these programs usually were harmless, boastful programming challenges or pranks between anonymous users. For example, the first computer virus—the Creeper Virus—simply displayed the message, “I’m the Creeper: Catch me if you can!” Shortly after its release, the Reaper—the first antivirus program—removed the Creeper Virus. In 1988, however, the Morris Worm demonstrated the potential for widespread harm by infecting ten percent of computers connected to the Internet. It was not long before states began using malware as a method of attacking adversaries in what is now known as a cyber attack.

B. WHAT IS CYBER WARFARE?

---

41 Id.
43 Id.
As developed nations become reliant upon computer systems in every sector of society, opportunities increasingly arise for adversaries to strike inexpensively, remotely, and effectively with little risk. For that reason, states and non-state actors turn to cyberspace to conduct warfare with greater frequency. This Section explores cyber warfare’s theater of conflict as well as the definition of a cyber attack in relation to cyber warfare, cybercrime, and other hostile actions taken online.

1. CYBER WAR’S “THEATER OF CONFLICT”

An integral aspect of evaluating cyber warfare’s legal status is determining the active “theater of conflict.” If an attack occurs within the active theater of conflict, the law of armed conflict governs. But when a conventional attack occurs outside of the geographically limited theater of conflict, it is less clear how the laws of war apply.45

The challenge in defining the theater of conflict in cyberspace is that any particular operation will instantaneously cross components of the Internet infrastructure, which is spread throughout multiple countries. Thus, defining the theater of conflict is not as simple as equating cyberspace infrastructure to other forms of civilian or military infrastructure.46 Fortunately, neither law nor custom supports confining a conflict to geographical boundaries. Such a constraint becomes dangerously illogical in conflicts that inherently cross borders.

---


Cyber warfare also allows combatants to fight from extreme distances, which raises a number of ethical and moral considerations. Not unlike the concerns raised in relation to those operating Predator drones, cyber attackers are far from the battlefield. Being removed from the horrors of war, cyber attackers risk becoming emotionally detached from the effects of their attacks, increasing the possibility of unnecessary harm, suffering and collateral damage.

However, while such ethical and moral considerations warrant exploration, the laws of war do not present additional restraints in this respect. For example, international law does not differentiate between hand-to-hand combat and an intercontinental ballistic missile. Similarly, cyberspace should be treated like any other theater of conflict regardless of its expanse or the location of those participating in cyber attacks.

2. DEFINING CYBER WARFARE

The all-encompassing term “cyber war” is not an apt description for hostile actions in cyberspace because of the wide range of possible intended effects of an attack. It is helpful to be more specific by distinguishing between cyber attacks and cyber exploitation.

The only international agreement that approaches a definition for cyber attacks is the Council of Europe’s Convention on Cybercrime—a multilateral treaty that increased cooperation among signatories to combat cyber crimes such as fraud, child pornography,

---

and copyright infringement.\textsuperscript{48} Because the Convention has not been widely adopted, it is not binding as customary international law.\textsuperscript{49} But the Convention demonstrates that international concern exists regarding the use of cyber attacks, and it recognizes a state’s duty to prevent these attacks. The treaty aims to harmonize the domestic criminal laws of the signatory states, including adoption of appropriate legislation to criminalize the enumerated cyber offenses. Most relevant for cyber attacks are the Convention’s provisions on data and system interference. The Convention requires signatories to adopt laws that criminalize “the damaging, deletion, deterioration, alteration or suppression of computer data without right,”\textsuperscript{50} as well as “the serious hindering without right of the functioning of a computer system” by similar means.\textsuperscript{51} While the Convention falls short of regulating cyber attacks, its incipient efforts at defining cyber attacks at an international level is significant.

The Department of Defense has not yet defined cyber warfare.\textsuperscript{52} But one workable definition of a cyber attack offered by the US Army’s DCSINT Handbook No. 1.02 is: “The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or

\textsuperscript{48} Council of Europe, Convention on Cybercrime art. 4, \textit{opened for signature} Nov. 23, 2001, E.T.S. No. 185.
\textsuperscript{50} Id.
\textsuperscript{51} Id. art. 5.
to intimidate any person in furtherance of such objectives.”53 The methodology of a cyber attack involves a deliberate action taken to “alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks.”54 Often, cyber attackers intend to destroy the entities reliant on a computer system or network rather than the computer system or network itself.55

By comparison, cyber exploitation is the use of a deliberate cyber action that seeks to extract confidential information from an adversary’s computer system or network.56 The goal of cyber exploitation is to obtain information from a computer network without the user’s knowledge, which amounts to a modern form of espionage. Espionage is illegal under the domestic laws of most nations, but it is not illegal under international law.57

Throughout history, nation-states have undertaken espionage by using agents to infiltrate and collect information about adversaries. Now, states can obtain the same information without the risk and complexity associated with using agents. Just as cyber

56 Id. at 81.
57 Roscini, supra note 8 at 93.
criminals use computer systems to enhance their illicit activity, so have state governments. (As one intelligence expert wrote, if you want to keep a secret, don’t write it down.58 The modern twist might be, if you want to keep a secret, don’t make it digital.) Cyber espionage, defined as the “unauthorized probing of a target computer’s configuration to evaluate its system defenses or the unauthorized viewing and copying of data files,” is a low-cost and low-risk tool for state governments.59 Using the same techniques that cyber criminals utilize for gaining confidential information—such as malware,
phishing,60 and code injection61—state governments now engage in for intelligence and commercial espionage.62

Anecdotal evidence suggests that cyber espionage is a familiar practice among state governments. Electronic trespassers probe US defense networks thousands of times each day.63 Israel is particularly direct about its exploration of cyber

60 Typically, the cyber attacker sends spam E-mail that appears to come from a legitimate user or institution. The spam E-mail urges the recipient to click on a link, which leads the user to a fraudulent website designed to look legitimate or innocuous. When the user enters confidential information, the fraudulent website records the information the recipient enters and sends it back to the attacker. See KELLIE BRYAN ET AL., CYBER FRAUD: TACTICS, TECHNIQUES, AND PROCEDURES 27 (James Graham et al. eds., 2009).

61 Code injection exploits a bug in computer program. An attacker injects code into a computer program to change its execution. Cyber criminals use vulnerabilities in commercial websites to introduce their own commands that will give them access to confidential information in the databases of websites. Most commonly cyber criminals target credit card information and social security numbers. Theoretically, a cyber attacker could employ a similar attack on “secure” databases that are connected to a government website. See James Verini, The Great Cyberheist, N.Y. TIMES, Nov. 10, 2010, http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?_r=2&scp=1&sq=alberto%20gonzalez&st=cse.

62 Corporations regularly report data breaches. These reports show that the cyber espionage direct efforts both at corporations with classified national security contracts and companies with proprietary information, seeking to obtain a competitive edge in the global economy—a security risk in its own right. In 2009, President Obama estimated that, “last year alone, cyber criminals stole intellectual property from businesses worldwide worth up to one trillion dollars.” President Barack Obama, Remarks by the President on Securing Our Nation’s Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

espionage tactics. The Israeli Defense Forces’ chief of military intelligence Major General Amos Yadlin explained that “[u]sing computer networks for espionage is as important to warfare today as the advent of air support was to warfare in the 20th century.”64 Since at least 2002, China has directed cyber espionage toward the United States in what the Department of Defense has termed Operation Titan Rain.65 One report states that China has already downloaded at least ten terabytes of data from the Non-classified Internet Protocol Router Network.66 Ten terabytes is enough space to store the entire printed collection of the Library of Congress in digital format. Additionally, cyber exploitation can serve as a modern form of reconnaissance that lays the groundwork for other forms of attack.

Nevertheless, cyber espionage and exploitation fails to rise to the level of warfare because the purpose or outcome of both cyber espionage and exploitation is to monitor information and not to affect a computer system’s functionality. The possibility of using cyber exploitation as a precursor to a cyber attack raises a separate set of legal questions beyond the scope and purpose of this Article. Although similar to traditional espionage in that cyber espionage may violate any number of domestic laws or international agreements, it does not violate international laws of war. Therefore, as used here, “cyber attacks” will not refer to espionage or reconnaissance performed via cyber exploitation.

65 KRAMER, supra note 59, at 85.
66 Id.
II. THE LAWS OF WAR IN CYBERSPACE

The laws of war provide the framework for when it is acceptable to resort to the use of force (jus ad bellum) and governs the limits of acceptable wartime conduct (jus in bello). Together, international treaties and customary international law articulate the principles that nations rely upon to determine the lawfulness of their forceful conduct. The first section has two parts and examines the framework of jus ad bellum to assess (1) whether cyber attacks violate the general prohibition on the “use of force” under Article 2(4) of the United Nations (UN) Charter, and (2) whether a cyber attack can reach the threshold of “armed attack” that triggers the right to self-defense under Article 51. The second section examines the consequences under international law of hostile cyber operations that do not rise to the level of an armed attack. The final section evaluates the jus in bello regime, which governs the conduct of warfare, to determine how cyber attacks should operate under the law of armed conflict.

A. JUS AD BELLUM—RE COURSE TO FORCE

1. DO CYBER ATTACKS VIOLATE THE GENERAL PROHIBITION ON THE USE OF FORCE?

Article 2(4) of the UN Charter declares that “[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”67 Determining whether a cyber attack violates this general prohibition on the use of force requires an understanding of 1) how force is interpreted in international law, and 2) whether cyber

67 U.N. Charter art. 2, para. 4 (emphasis added).
attacks can reach the appropriate level under those standards.  

One place to begin this analysis is the Vienna Convention on the Law of Treaties, which provides the rules of treaty interpretation. Although adopted after the Charter, international law experts generally agree that the Convention’s rules reflect customary international law.

Article 31 of the Convention states that “[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.” The ordinary meaning of “force” is broad and encompasses conventional notions of kinetic attacks as well as other coercive measures. Other coercive measures include: financial instruments, i.e., granting or withholding economic indulgences from a target; diplomatic instruments, i.e., negotiation and advocacy

---

68 Even if a cyber attack does not rise to the level of force prohibited under Article 2, a cyber attack may still be inconsistent with international law. Massive Distributed Denial of Service (DDoS) attacks that target the business, government and commercial sectors of an adversary for a political purpose certainly constitute a prohibited intervention. See infra notes 83–85 and accompanying text. The International Court of Justice states that “[t]he principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference . . . it is part and parcel of customary international law.” See also Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27) (observing that the UN Charter does not cover the whole area of the regulation of the use of force).


71 Black’s Law Dictionary defines “force” as “power, violence, or pressure directed against a person or thing.” BLACK'S LAW DICTIONARY 717 (9th ed. 2009).
between state representatives; and ideological or propagandistic instruments, which deploy carefully selected signs and symbols to relevant sectors of society with the design of influencing the governing elite.  

Under a broad reading of “force,” each of these instruments—military, economic, diplomatic, and ideological—could be subject to regulation under the Charter.

However, in light of the “object and purpose” of the Charter, “force” should be read more narrowly. The express aim of the United Nations is to maintain international peace and security, as well as “to save succeeding generations from the scourge of war.” That suggests the notion of force in 1945 was limited to the military instrument. The drafting history of the Charter reinforces this conclusion. The travaux préparatoires shows that a proposal was submitted to extend the scope of Article 2(4) to other strategic instruments—specifically, to economic coercion. The United Nations ultimately rejected this proposal. By explicitly excluding economic coercion from the definition of force in the drafting of Article 2(4), and implicitly rejecting ideological and diplomatic instruments as well, the drafters signaled that the determination of whether a nation has used force in violation of Article 2(4) focuses only on military instruments.

However, concluding that the Charter embraces a relatively narrow meaning of “force” does not end the analysis. Because the International Court of Justice (ICJ) has stipulated that the Charter does not encompass the

---

73 U.N. Charter pmbl.
74 See Doc. 2, G/7 (e)(4), 3 U.N.C.I.O. Docs. 251, 252–53 (May 6, 1945) (Brazilian amendment proposals).
75 See Summary Report of Eleventh Meeting of Committee I/1, Doc. 784, I/1/27, 6 U.N.C.I.O. Docs. 331, 334, 559 (June 4, 1945).
whole area of the regulation of force, and that it is appropriate to turn to customary international law to determine the regulation of force as well, this Article also references international agreements and decisions of the international court to discern how force is regulated under customary international law.\footnote{Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. US), 1986 I.C.J. 14 (June 27) (observing that the United Nations Charter, the convention to which most of the United States’ argument is directed, does not cover the whole area of the regulation of the use of force in international relations because customary international law continues to exist alongside treaty law).}

Cyber weapons are versatile and can be either a supporting actor in the theater of conflict or the main event. They are not monolithic weapons whose use leads to straightforward answers about whether they violate the prohibition on force. Rather, the innumerable harmful effects caused by cyber attacks make their categorization both more complex and more necessary. The effects of a cyber attack can range from a simple inconvenience (such as a DDoS attack that disrupts web traffic temporarily), to physical destruction (such as changing the commands to an electrical power generator causing it to explode), and even to death (such as disrupting the emergency lines to first responders so that calls cannot be made to police or ambulance services). But treating all forms of cyber attack as a use of force would require an implausibly broad reading of Article 2(4) that includes non-physical damage. A more nuanced approach is needed.

Another challenge is that the intensity and temporal scope of a cyber attack can transform an event from a low-level aggressive act to a prohibited use of force. In Arm\textit{ed Activities on the Territory of the Congo,} (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, 165 (Dec. 19), the ICJ determined that a violation of Article 2(4) resulted from the “magnitude and duration” of
Uganda’s actions.⁷⁷ Therefore, magnitude and duration of an attack are appropriate factors for consideration in any model that analyzes the coercive tactics employed by a state. Beyond these factors, several possible models exist for determining whether a cyber attack rises beyond mere coercion to a use of force.

The first approach to analyzing force is to examine the method of delivery. Under this model, cyber weapons are categorized by the specific method of delivering an attack on an adversary. Whether it is a virus, worm, network intrusion, or some other cyber attack, this model prohibits cyber attacks based on how they are executed. The severe damage that particular types of cyber attack can inflict worldwide relative to the limited effects of narrowly designed exploits provides the basis for this approach. Of course, certain cyber weapons are inherently more destructive and dangerous than others. Under conventional warfare, specific treaties have already emerged around atomic, biological, chemical, and nuclear weapons. A convention that specifically regulates cyber weapons would be the natural evolution of weapons treaties. The challenge a cyber weapon-specific approach faces is that technology changes quickly; any international agreement deeming a particular type of cyber attack unlawful might be outdated by the time it is ratified.

The second approach to analyzing force views cyber weapons under a strict liability model. Adherents to this model deem any use of cyber attacks against

---

⁷⁷ Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, 165 (Dec. 19) (“The unlawful military intervention by Uganda was of such a magnitude and duration that the Court considers it to be a grave violation of the prohibition on the use of force expressed in Article, 2 paragraph 4, of the Charter.”).
critical infrastructure to be a use of force. \(^{78}\) Many nations have already audited their critical infrastructure to determine where they are vulnerable to the consequences of a cyber attack. \(^{79}\) The next step would be to authorize self-defense against cyber attacks that target critical infrastructure. Proponents of strict liability argue that it is an appropriate model because of the instantaneous and destructive nature of cyber attacks. Once a cyber attacker has targeted critical infrastructure, an imminent threat exists that, at least arguably, creates a sufficient level of harm to justify anticipatory self-defense.

The weakness of this model is that the effects of cyber attacks may be indiscriminate and uncontrolled once unleashed. Cyber attacks do not always intentionally target the critical infrastructure that they eventually disrupt. And even if a cyber attack targets critical infrastructure, such as the banking and finance system, the strict liability approach introduces interpretive difficulties by collapsing the distinctions between armed violence, coercion, and interference. Even more troubling is that a strict liability model would authorize self-defense for the most benign offenses.

The third approach to analyzing force examines cyber attacks as instruments equivalent to traditional kinetic weapons by looking at the direct results of an attack. If the result would be considered a prohibited use of force when caused by a kinetic weapon, then a cyber

---

\(^{78}\) Walter Gary Sharp Sr., CyberSpace and the Use of Force 129-31 (1999).

\(^{79}\) The United States, for example, has outlined several types of infrastructure—the physical and cyber assets of public and private institutions in agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance chemicals and hazardous materials, and postal and shipping—the destruction or incapacity of which would cripple the nation’s defensive or economic security. Roscini, supra note 8, at 117.
A cyber attack is a use of force if the attacker seeks to cause direct physical destruction, injury, or death. This approach removes the need to examine the instrument of delivery, and it allows the international community to adapt the Charter to evolving technology while accounting for nuances in the intensity of a cyber attack.  

The flaw in this approach is that most cyber attacks do not directly cause physical damage or death. For example, a cyber attack that temporarily shuts down the communication lines for emergency police and ambulance services may not cause physical damage or deaths directly, but it could easily cause both indirectly. Drawing the line between direct and indirect effects of a cyber attack is extremely difficult.

Michael N. Schmitt posits a model that has gained traction among legal scholars. Schmitt advocates for a consequence-based approach. This framework requires examining whether the reasonably foreseeable consequences of a cyber attack resemble the consequences of a conventional attack. Schmitt provides six criteria for evaluating the consequences of cyber attacks on the target state: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. If the cyber attack shares enough commonalities in the six factors, extension of the prohibition on force is justified. The benefit of this model is that it addresses how to evaluate cyber attacks.

---

80 Ian Brownlie, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362 (1963). This method also allows for the characterization of chemical and biological weapons as a use of force under the Charter despite the cause of injury and death from those weapons not being a kinetic result of the instrument.

that are coercive but do not directly result in physical damage, injury, or death.

Consider two examples from the widely reported Russian cyber attack on Estonia. During World War II, the Soviet Union placed a bronze memorial statue in Tallinn, Estonia. Estonians today view the statue as a symbol of Soviet occupation and political repression, while ethnic Russians in Estonia see the statue as a tribute to fallen Soviet soldiers. In April 2007, the Estonian authorities decided to remove the controversial statue. The result of this decision was two nights of mass protests and riots in Estonia known as “Bronze Night.” In the weeks following Bronze Night, Estonia’s digital infrastructure experienced a massive cyber attack originating mostly in Russia. Russian “hacktivists” used massive DDoS attacks to target Estonia’s web servers and bring web traffic to a halt. Specific targets included news and government websites.

Under Schmitt’s criteria, the severity of this cyber attack falls short of the use of force. While the cyber attacks were immediate, the consequences were minimal. There was no physical damage or measurable suffering. The disruptions mostly caused a temporary inconvenience. The disruption of web traffic caused by the attack was indirectly related to the likely intended coercive effect, which was to reverse the Estonian government’s decision to remove the statue. The attack was intrusive and presumptively illegitimate, but the net results did not sufficiently resemble the use of force.

---

82 Hacktivists are also popularly called “patriotic hackers.”
One commentator astutely described the cyber attacks as being “more like a cyber riot than a military attack.”

There was, however, a cyber attack during this episode that brought down phone lines to emergency services, which presents a more troublesome scenario that jeopardized human life and limb. The severity of that cyber attack has consequences equivalent to a use of force. What matters in that cyber attack is not that it potentially inflicted severe consequences, but that it was liable to produce such consequences. It can be assumed that the result of the cyber attack was immediate and created a measurable level of suffering for those who were not able to access police or ambulances in an emergency. In that instance, the cyber attack should rise to the level of force under Schmitt’s framework despite the indirectness of its consequences.

These Bronze Night examples demonstrate that a consequence-based model is flexible enough to distinguish between different levels of attacks within the same conflict. In one instance, the consequence-based approach finds that a cyber attack should be considered forceful enough to be unlawful under Article 2(4). In the other, the consequences are too minimal to rise to the level of force. This model accounts for the nuances of a cyber attack’s intensity without ignoring the indirect effects of a cyber attack. By comparison, under the text of the Charter alone, neither cyber attack amounts to a prohibited use of force.

---


The deficiency of Schmitt’s approach is that extending its principles outside the regime of cyber weapons introduces measures of coercion not traditionally included in the prohibition on force, such as economic, diplomatic, or ideological coercion. An alternative approach might be to scrap the Schmitt model altogether when the targets are economic, diplomatic, and ideological instruments of the state, which is not without precedent given that the Charter does something similar. (In the Charter, the military instrument is presumptively forceful in Article 2(4), leaving out the economic, diplomatic, and ideological modes of coercion.)

Another criticism of the Schmitt model is that it offers little guidance as to the weight of each of the six factors. Such indeterminacy will lead to variance in the rules of engagement in cyberspace. One way to slightly modify the Schmitt model is to tier the factors. For example, presumptive legitimacy should be a first-tier factor. Once a state has determined that an attack is not a legitimate use of force, the next tier to consider would be the severity and invasiveness of the attack. Following this, the immediacy, directness, and measurability of an attack would help a state determine whether a cyber attack is a prohibited use of force.

Because cyber attacks are so versatile and variable in their methods and purposes, a unilateral approach to regulation leaves much to be desired. There is no perfect method for analyzing cyber attacks with current technology. Effects-based models require a post-hoc analysis that may take days, weeks, or longer to determine the extent of an attack, which is an unacceptable timeframe for responding to an equivalent kinetic attack. But a strict liability model raises the possibility of wrongly escalating force in response to a low-level cyber attack. Technologies to
identify and assess cyber attacks in real-time may eventually make this a moot point. Until then, classifying a cyber attack by a degree of force is only one of many hurdles for decision makers.

2. DOES A CYBER ATTACK REACH THE THRESHOLD OF “ARMED ATTACK” THAT TRIGGERS THE RIGHT TO SELF-DEFENSE UNDER ARTICLE 51 OF THE UN CHARTER?

When there is a conflict between nations, the Charter demands that members “[s]ettle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.” Thus, the authority for a state’s use of force originates either from the UN Security Council or by the state’s right to act in individual or collective self-defense. The lingering question is whether cyber attacks can reach the threshold of “armed attack” that triggers the right to self-defense under Article 51 of the Charter. Article 51 states:

Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.

Is there a difference between an “armed attack” under Article 51 and a “use of force” under article 2(4)? Some scholars argue that any use of force by regular armed forces constitutes a per se armed attack.

---

86 U.N. Charter art. 2(3).
87 U.N. Charter art. 51 (emphasis added).
Under this view, any offensive action by a military cyber unit is an armed attack because it emanates from the armed forces of a state. The United States, China, Iran, Israel, and other nations around the world have already established military cyber units. Offensive actions by these cyber units would be considered a *per se* armed attack that triggers the right to exercise individual or collective self-defense. The danger is that a single errant soldier could embroil a nation in a protracted conflict if his or her action permits the target state to respond in self-defense. But this danger also exists outside the realm of cyberspace, so this concern represents a difference in degree rather than kind.

Others reject the *per se* approach, arguing that the ICJ’s “scale and effects” test is more appropriate to determine when Article 51 is triggered. This is consistent with the ICJ’s position that there is a substantive distinction between the “use of force” and an “armed attack.” In *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. US)*, 1986 I.C.J. 14, 202 (June 27), the ICJ defined the difference as primarily one of “scale and effects.” Thus, not every use of force warrants the exercise of the right of unilateral self-defense. To know whether a cyber attack meets the threshold of “armed attack” requires knowing

---

89 Roscini, *supra* note 8, at 97-98.

90 Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, 214 (Dec. 19) (“According to a well-established rule of a customary nature, as reflected in Article 3 of the Fourth Hague Convention respecting the Laws and Customs of War on Land of 1907 as well as in Article 91 of Protocol I additional to the Geneva Conventions of 1949, a party to an armed conflict shall be responsible for all acts by persons forming part of its armed forces.”).

where the de minimis threshold lies. However, this is a vague and fact-specific rule.

Under such a regime, interpretive power shifts to institutional bodies such as the United Nations and the ICJ. Perhaps it is ideal to involve the international community in determining whether a nation can rightfully respond in self-defense. But the “scale and effects” test also leaves a targeted state less guidance to determine whether an armed response is lawful.

Regardless of the scale or effect of an attack—whether it is kinetic or cyber—the type of weapon used in an “armed” attack is immaterial. In an advisory opinion concerning nuclear weapons, the ICJ referred to Articles 2(4) and 51, stating that “[t]hese provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed.”92 The Security Council reaffirmed this sentiment when it authorized the United States to respond forcefully in self-defense to the 9/11 attacks, where the “weapons” were hijacked airplanes. Thus, under the “scale and effects” test, a cyber attack could lawfully trigger the right of self-defense under Article 51 if it inflicts substantial destruction upon important elements of the target state.

So where does the de minimis threshold lie? Customary practice suggests that under conventional notions of force, even small-scale bombings, artillery, naval or aerial attacks qualify as “armed attacks” activating Article 51, as long as they result in, or are capable of resulting in, destruction of property or loss of lives.93 By contrast, the firing of a single missile into some unpopulated wilderness as a mere display of force

92 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8).
would likely not be sufficient to trigger Article 51, despite violating Article 2(4).

What would the firing of a missile into unpopulated wilderness equate to in cyberspace? A cyber attack that merely creates an inconvenience might be a prohibited use of force, but it would not rise to the level of an armed attack. In comparison, a cyber attack capable of substantially destroying property or causing the loss of lives should trigger the right to self-defense.

Modern weapons—such as cyber weapons—have created new complications for states attempting to comply with the self-defense exception of the Charter. For example, when the Charter was written, weapons of mass destruction had yet to be developed. First strikes were incapable of the widespread destruction enabled by modern weapons. Today, states faced with strict compliance to Article 51 run the risk of total annihilation. Thomas M. Franck—a notable international law scholar—criticized the irrationality of the Charter’s requirements, writing that “[t]aken literally, Articles 2(4) and 51 together seem to require a state to await an actual nuclear strike against its territory before taking forceful countermeasures. If this is what the Charter requires, then, to paraphrase Mr. Bumble, the Charter is ‘a ass.’”94 As Franck suggests, it is unreasonable to expect a state to comply with the Charter to the point of its total destruction.

The prospect of total or significant destruction has led states to turn to customary international law for the determination of when it is appropriate to forestall an attack. Under customary international law, anticipatory self-defense is a legitimate preemptive strategy. The *Caroline* test formulates the customary understanding of

---

anticipatory self-defense. It states that for an action of anticipatory self-defense, a state must show that the “necessity of self-defense was instant, overwhelming, leaving no choice of means, and no moment of deliberation.”95 Even where each condition is met, forceful actions of anticipatory self-defense cannot be “unreasonable or excessive; since the act, justified by the necessity of self-defense, must be limited by that necessity, and be kept clearly within it.”96

Sophisticated cyber attacks are designed to overwhelm a target state’s computer systems instantaneously. There are, of course, cyber attacks that a state might foresee and counteract. A state might discover evidence of a cyber attacker’s attempted network intrusion, an audit of computer systems might reveal unauthorized backdoors or malware, or targeted states might uncover an online forum that serves as a gathering place for hacktivists to trade information and tools prior to a coordinated attack. In such cases, the target state is previously aware of a planned cyber attack and may invoke its right to respond in anticipatory self-defense if the Caroline test criteria are met. Where met, a state might lawfully disable the servers that host the online forum where cyber attackers are gathering, assuming the state has no other means by which to forestall the imminent attack.

3. ATTRIBUTING STATE RESPONSIBILITY

Before a state responds in self-defense, several considerations must be weighed. One issue is whether the cyber attack should be treated as a law enforcement matter or a national security matter. Relevant to this determination is whether the level of force used in the cyber attack rises to that of an armed attack, as discussed

96 Id.
in Section II(a)(ii). Another consideration is whether the state whence the attack originated is complicit. If the act of self-defense is not in immediate response to an ongoing attack, the state must impute responsibility before launching its cross-border counter-attack. Establishing state responsibility in the area of cyber attacks requires understanding states’ duties to one another, particularly regarding non-state actors operating within their jurisdiction.

In 2001, the International Law Commission issued the Draft Articles on State Responsibility, which articulates the international jurisprudence on state responsibility. Article 1 states that “[e]very internationally wrongful act of a State entails the international responsibility of that State.”97 This notion of state responsibility is supported by state practice as well as opinio juris. In the Corfu Channel Case, (U.K. v. Alb.), 1949 I.C.J. 4 (Apr. 9), the ICJ examined the threshold to attribute responsibility for actions within a state’s borders.98 The ICJ held that territorial sovereignty is not only an essential foundation of international relations, but also that under customary international law, every state also has an obligation “not to allow knowingly its territory to be used for acts contrary to the rights of other states.”99 This formulation, however, does not account for the subtleties in degree of state responsibility. Should a state be held internationally responsible for a single soldier or patriotic hacker that uses a cyber attack to destroy critical infrastructure of an adversary? These questions merit further exploration.

99 Id. at 22.
i. State Actors

There is little controversy that, if a state’s agent attacks another state, then the hostile conduct is attributable to the state. Article 4 of the Draft Articles on State Responsibility declares that “[t]he conduct of any State organ shall be considered an act of that State under international law.”\(^{100}\) A state organ is understood to be all the individual or collective entities that make up the organization of the state and act on its behalf.\(^{101}\)

This principle is a codification of customary international law. It reflects the assumption that a state is fully responsible for its agents—even when those agents act outside the scope of their duties. In *Armed Activities on the Territory of the Congo*, (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, 214 (Dec. 19), the ICJ held that “[a]ccording to a well-established rule of a customary nature . . . a party to an armed conflict shall be responsible for all acts by persons forming part of its armed forces.”\(^{102}\) This rule also applies to a person or entity that is not an organ of the state but nevertheless exercises elements of governmental authority.\(^{103}\) This extends to private or public entities that a state may charge with elements of authority normally associated with the government. For example, if the British government employs private defense companies and

\(^{100}\) State Responsibility, *supra* note 97, at art. 4.

\(^{101}\) *Id.* art. 2 commentary.

\(^{102}\) Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, 214 (Dec. 19) (“According to a well-established rule of a customary nature, as reflected in Article 3 of the Fourth Hague Convention respecting the Laws and Customs of War on Land of 1907 as well as in Article 91 of Protocol I additional to the Geneva Conventions of 1949, a party to an armed conflict shall be responsible for all acts by persons forming part of its armed forces.”).

\(^{103}\) State Responsibility, *supra* note 97, at art. 5, 8; *see* Hyatt Int’l Corp. v. Iran, 9 Iran-U.S. C.T.R. 72, 88-94 (1985).
authorizes them to conduct active defense measures, the conduct of the private defense company is imputed to Britain. As the Commentary to the Draft Articles on State Responsibility notes, “[i]f it is to be regarded as an act of the State for purposes of international responsibility, the conduct of an entity must accordingly concern governmental activity and not other private or commercial activity in which the entity may engage.” 104 This formulation is consistent with the “effective control” test discussed earlier. Similarly, a state may not coerce another state to do its bidding without accountability. Article 17 of the Draft Articles on State Responsibility holds a state internationally responsible for wrongful acts that “it directs and controls another State in the commission of,” if the state exercising the direction and control does so knowingly. 105 This test hearkens back to the era of the Corfu Channel Case and its mandate that a state not knowingly allow an attack to originate from its territory. This is particularly important in the area of cyber attacks because of their surreptitious and uncontrollable nature.

As mentioned, many states have already begun developing cyber units within their military or intelligence apparatuses. States have also delegated some elements of their cyber attack capabilities to the private sector. One state might even consider using another state to launch an attack on its behalf. Although tracing a cyber attack is a formidable technical challenge, if the target state successfully traces a cyber attack to the source state’s cyber unit or to an entity acting with the authority or under the control of the source state, the latter ought to be held responsible.

104 State Responsibility, supra note 97, at art. 5.
105 Id. at art. 17.
ii. *Non-State Actors*

A harder question, in both the realm of cyberspace and traditional warfare, is determining whether it is appropriate to attribute state responsibility when non-state actors perpetrate an attack. Article 51 of the Charter does not provide instruction on whether a state may respond with force to a non-state actor. Non-state actors, usually hacktivists, present a complicated issue for targeted states.

Hacktivists are usually private citizens motivated by nationalistic or ideological feelings who possess sufficient skill to participate in a cyber attack. The nature of cyberspace permits hacktivists to launch attacks on from anywhere, at will, without government direction. Hacktivists’ freedom to engage in cyber attacks from virtually anywhere in the world allows them to operate from the territory of a third party. Any action taken against a hacktivist in the territory of a third party state raises questions about violating that state’s sovereignty, as well as whether the third party state has certain rights and obligations. The Charter does not explicitly address this facet of international conflict, leaving a legal loophole that hacktivists might exploit.

Yet custom and practice demonstrate that states can—and do—respond with force to non-state actors. The international response to the 9/11 attacks on the United States validated this principle of customary international law. After 9/11, the Security Council passed Resolution 1368, which reaffirmed the “inherent right” of the United States to respond in self-defense in accordance with Article 51 of the UN Charter.106 Weeks later, when it was clear that non-state actors had committed the 9/11 attacks, the United States still

---

received nearly universal support, including from the Security Council, when it invoked its right to respond in self-defense.  

On what basis do we attribute responsibility to a state for the actions of its non-state actors? If the state directs or controls the non-state actors, regardless of whether the non-state actors are within its jurisdiction, there are several bases for which to hold the state responsible. However, “lone wolf” hacktivists—those who act without endorsement of the state—are a different matter.  

Under the original Corfu Channel formulation, if a state may not knowingly allow its territory to be used for acts that violate another state’s rights, then mutatis mutandis a state may not knowingly allow non-state actors within its borders to attack another state. More recently, the Articles on State Responsibility augment the Corfu Channel test by imputing responsibility to a state if “the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.”

The Articles on State Responsibility articulates the rule of the Nicaragua case. In Nicaragua, the issue brought before the ICJ was whether the United States was responsible for the actions of the contra guerillas in their rebellion against the Nicaraguan government. The Court held that to find the United States responsible would require “effective control” over the non-state actor group and also the exercise of that control with respect to the specific operation in which breaches were committed. Such a finding would imply that state

---

108 State Responsibility, supra note 97, at art. 8 (emphasis added).
control extends beyond its immediate territory. Thus, if a state is in “effective control” of non-state actors operating in another territory, it may be held responsible for their actions. The Declaration on the Strengthening of International Security proclaims that every State has the duty to refrain from organizing, instigating, or participating in acts of civil strife or terrorist acts in another state. Under this standard, if a state organized, assisted, and controlled hacktivists as proxies, responsibility for their agents’ actions is imputed to the state with respect to the specific operations “controlled” by the state, wherever they might occur.

On the other hand, the International Criminal Tribunal for the Former Yugoslavia articulated a lower “overall control” test in Prosecutor v. Tadic, Case No. IT-94-1-T, Sentencing Judgment, ¶ 120 (July 14, 2007). The Tadic tribunal acknowledged that this standard “to some extent equates the group with State organs proper.” The Tadic standard was applied only to participants in an organized and hierarchically structured group, such as a military or paramilitary force.

An example of such a paramilitary group is the Russian Business Network, which is often associated with Russia’s political and military elite, though it is not a formal participant. The Russian Business Network was intimately involved in the cyber attacks on Estonia and Georgia, attacks for which Russia denied its own

110 Prosecutor v. Tadic, Case No. IT-94-1-T, Sentencing Judgment, ¶ 120 (July 14, 2007). This lower standard was criticized by the ICJ in the Genocide Case as being unsuitable because it “has the major drawback of broadening the scope of State responsibility well beyond the fundamental principle governing the law of international responsibility.” Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43 (Feb. 26).

111 Tadic, Case No. IT-94-1-T, at ¶ 121.
involvement. Under the “overall control” test, the relationship between the Russian Business Network and the Russian State should be sufficient to impute state responsibility.

As for individuals and unorganized groups, the Tadic tribunal accepted the higher “effective control” standard to impute state responsibility. In order to meet the “effective control” test, the Tadic tribunal determined that there must be “specific instructions or directives aimed at the commission of specific acts,” or, in the absence of direction, that there be a public endorsement of the acts ex post facto.\(^\text{112}\) Article 11 of the Draft Articles on State Responsibility declares that “[c]onduct which is not attributable to a state under the preceding Articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.”\(^\text{113}\)

The United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3 (May 24), case is evidence of this principle in practice. The seizure of the US embassy and its personnel by militants was endorsed by the Iranian State. The ICJ held that Iran’s approval translated into state responsibility for the actions of the militants. Under this framework, if individuals or unorganized groups of hacktivists use a cyber attack to destroy a power plant in another state and their host state unequivocally approves the action, the attack will be imputed to that host state.

The hardest question for state attribution is whether a state is responsible for lone wolf hacktivists that operate without active encouragement from a state. In this scenario, international law requires states to take reasonable preventive measures. The Convention on

\(^{112}\) Id. at ¶ 132.

\(^{113}\) State Responsibility, supra note 97, at art. 11.
Cybercrime, for instance, requires signatories to adopt domestic laws that criminalize cyber attacks. How far a state’s duty extends to prevent lone wolf hacktivists remains undetermined. For instance, must a state adapt its technology in some way, for example by removing online anonymity? Such a requirement raises serious questions about the liberty and privacy interests of individuals. But this is an issue that is more clearly within the range of domestic law, rather than the laws of war, and thus outside the scope of this Article.

What if a state were required by international law to take reasonable measures to protect other states from foreseeable cyber attacks? Under that standard, a state that knows of cyber attackers launching attacks must take reasonable steps to fulfill its duty, by stopping the attacks, bringing the attackers to justice, or preventing further attacks. If a state does not cooperate, the targeted state may respond unilaterally in self-defense under Article 51. If a state knowingly allows—either through action or omission—a non-state actor to commit an attack, the state would be held internationally responsible. But if the state undertakes sufficient measures to protect other states, and a cyber attack still manages to originate from its territory, the state would not be responsible.

Since the 9/11 attacks, scholars argue that there has been a shift in the doctrine on state responsibility. Arguably, pre-9/11, a state would be held responsible for the actions of hacktivists operating within its territory if it could be shown that the state exercised “effective control” over them. State responsibility did not extend to knowingly harboring perpetrators of attacks. Since 9/11,

---
this understanding of state responsibility has been challenged. Evidence of this change is seen in the overwhelming international support for the US campaign against Al-Qaeda.\textsuperscript{115} This change is perhaps best encapsulated by the Security Council’s adoption of Resolutions 1368 and 1373.\textsuperscript{116} In Resolution 1368, the Security Council explicitly stated that those who aided, supported, or harbored the perpetrators of the 9/11 attacks would be held accountable.\textsuperscript{117}

This view of state responsibility remains controversial. It suggests a remarkable shift from the standards articulated in Nicaragua and Tadic. Those who dispute the shift in the doctrine of state responsibility claim that the Security Council resolutions were an exceptional response to an exceptional set of circumstances. Perhaps, however, the international response can also be explained on the grounds that harboring the perpetrators of the 9/11 attacks is similar to endorsing their actions, which implies that the state is knowingly in violation of its duty to prevent attacks from its territory.

This change puts a high burden on states in the realm of cyberspace without any direction as to compliance. Cyber attacks can be executed from virtually anywhere, meaning that every state could potentially be held internationally responsible, even where its only nexus to the attack was the attacker’s presence on its soil for the moment that it took to plug in and execute the attack.

Regardless of which standard is used, a state may not attribute state responsibility and then

\textsuperscript{115} Id. (discussing support for the American military campaign in Afghanistan).

\textsuperscript{116} S.C. Res. 1368, supra note 106; S.C. Res. 1373, supra note 107.

\textsuperscript{117} S.C. Res. 1368, supra note 106 (emphasis added).
immediately respond with force. Rather, the victim state must request that the offending state comply with its international obligations. If the offending state does not comply, the targeted state may impute state responsibility and act accordingly.

B. CYBER ATTACKS NOT COVERED BY JUS AD BELLUM

Cyber attacks that rise to the level of a prohibited use of force or that cross into the threshold of armed attack are regulated by *jus ad bellum*, which was designed to govern warfare. This Section, however, will examine how to regulate cyber attacks that fall below the level of a use of force and are consequently not covered by *jus ad bellum* protections. It is divided into two parts: the first part discusses cyber attacks that involve the use of economic, diplomatic, or ideological instruments. The second part examines low-intensity cyber attacks involving the use of the military instrument.

1. COERCIVE NON-MILITARY INSTRUMENTS IN CYBERSPACE

Low-intensity conflicts are conducted using the four strategic modes discussed previously: military, economic, diplomatic, and ideological. Regardless of whether these instruments are used as a tool of persuasion or coercion, their intended outcome is to influence the behavior of the targeted state. While the Charter deals primarily with the military instrument,

118 Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, 55-56 (Sept. 25) (“In the first place [countermeasures] must be taken in response to a previous international wrongful act of another State and must be directed against that State. . . . Secondly, the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it. . . . [Third] the effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question.”).
cyber attacks are versatile enough to fit within the other modes. This Section will examine the following scenarios using the non-military modes of coercion—economic, ideological, and diplomatic—and how international law might govern them:

Economic: A cyber attacker takes the New York Stock Exchange offline to undercut confidence in the integrity of the American financial markets.

Ideological: A cyber attacker manipulates the Internet pages of American politicians to associate them with radical positions with the intention of undermining their domestic political support.

Diplomatic: A cyber attacker steals classified cables from the US Department of State and publishes them online to embarrass the diplomatic corps of the United States.

i. The Economic Instrument

Hackers already appear to have penetrated into the computer systems that control the New York Stock Exchange.119 While no damage appears to have ensued, these breaches illustrate the extraordinary opportunity for economic devastation. A cyber attack undermining the international community’s faith in the financial markets would cause a vast economic disruption with worldwide ramifications. How might international law treat such an attack?

As previously mentioned, Article 2(4) did not categorize economic coercion as a prohibited use of force. Nowhere in the Charter is economic coercion prohibited. The Charter does, however, mention that

---

economic sanctions are permitted when called for by the Security Council.\footnote{U.N. Charter art. 41.}

In practice, economic coercion is an accepted tactic in international relations. States regularly use loans, credits, and foreign aid, among other means, to influence state action in designed ways. As will be discussed, economic coercion is also an lawfully accepted method of deprivation that states use as a countermeasure, also known as retorsions. While domestic laws may prohibit covert methods of economic coercion such as bribes or payments for intelligence, there is no comparable prohibition in international law. Some experts argue that economic modes of coercion are welcome when the alternative is to resort to military force.\footnote{Seid-Hohenveldern, \textit{The United Nations and Economic Coercion}, 18 BELGIAN REV. INT’L L. 9, 12 (1984).} Note that this does not mean that economic coercion is unregulated or ought to be lawful; extreme forms of economic coercion ought to be unlawful.

W. Michael Reisman and James Baker III offer one explanation for the unlawfulness of such an extreme method of economic coercion. \"[W]e would surmise that where the particular unilateral economic strategy raises costs as a means of securing desired behavior, it would be viewed as lawful. Where it would seriously undermine a political, economic or, if practiced widely, disrupt the international economic system, it would, like other undiscriminating strategies that injure unrelated parties, probably be viewed as unlawful.\"\footnote{REISMAN & BAKER, supra note 72, at 30 (emphasis added).} An action that would strike the heart of the American economy would certainly rise to an indiscriminate strategy that injures an unacceptable number of non-combatant parties.
ii. The Ideological Instrument

In previous cyber conflicts, cyber attackers have defaced the websites of political leaders as a form of psychological operation. The process of mischaracterizing politicians is regularly witnessed during election cycles. Would a state violate its international obligations by employing a cyber attack that discredited an American politician, e.g., by associating him or her with radical positions to undermine his or her support, thereby intervening in the United States’ political process?

The ideological instrument is an attempt by an external actor to influence the body politic of a state for the purpose of changing its behavior. The democratic nature of cyberspace makes it particularly vulnerable to the ideological instrument. Virtually anyone can access the Internet, allowing a message to gain widespread traction more easily than traditional measures of propaganda. The combination of the worldwide audience and the ease with which a cyber attacker can implant a message makes cyberspace a fertile ground for using the ideological instrument.

The ideological instrument presents a struggle between free speech and a state’s responsibility to promote non-interference in the affairs of other states. While the Charter is silent on the use of the ideological instrument as a method of coercion, a number of international agreements restrict or limit the use of the ideological instrument for hostile purposes.

The General Assembly has set forth its view of propaganda. In Resolution 110, the international body “condemns all forms of propaganda . . . which is either designed or likely to provoke or encourage any threat to the peace, breach of the peace, or act of aggression.”

---

Subsequent resolutions have also sought to proscribe conduct for “war mongering” and “hostile propaganda.”\textsuperscript{124} State practice, however, demonstrates that these resolutions have little to no effect on state conduct. Thus, the international community has not come to a workable resolution of the tension between a state’s promotion of domestic free speech and a state’s responsibility to adhere to the principle of non-interference.

There are several well-known convictions for violations of the prohibition on inciting violence through propaganda. Notably, these convictions arise in the context of genocide. In the Nuremberg Trials, the newspaper publisher and author Julius Streicher was convicted for a crime against humanity for inciting murder and extermination in World War II.\textsuperscript{125} In \textit{Prosecutor v. Jean Paul-Akayesu}, Case No. ICTR 96-4-T (Sept. 2, 1998), the International Criminal Tribunal for Rwanda determined that Akayesu intended to incite genocide against the Tutsi group in Rwanda.\textsuperscript{126}

Outside of genocide, the operational mode of international law as it relates to the ideological instrument is an \textit{ad hoc} approach more concerned with the method of communication and how it is controlled than the effect of its content. Thus, a cyber attacker that sought to influence the internal body politic of an adversary by manipulating the webpages of American politicians to associate them with radical positions is likely a lawful action under international law. The same

\textsuperscript{124} Declaration on the Inadmissibility of Intervention and Interference In the Internal Affairs of States, II(j); G.A. Res. 2625 (Declaration on Friendly Relations).

\textsuperscript{125} The Trial of German Major War Criminals: Proceedings of the International Military Tribunal Sitting at Nuremberg Germany, Part 22, 501-2 (1950).

\textsuperscript{126} Prosecutor v. Jean-Paul Akayesu, Case No. ICTR 96-4-T (Sept. 2, 1998).
action might nevertheless be unlawful under domestic criminal laws.

The action’s lawfulness does not stop a state from responding with proportional countermeasures to a hostile cyber attack, which could create tension between a state’s countermeasures and the promotion of free speech. The danger lies in the possibility that the internal elite will resort to a restriction on free communication when it is used to threaten their power. The potential threat to free speech should encourage a state to restrain itself in how broadly it interprets a cyber operation that involves the ideological instrument.

**iii. The Diplomatic Instrument**

The diplomatic instrument consists of communication among the elites of nation-states and international organizations. Operationally, elites conduct much communication in secret, without domestic or international appraisal. Although the end product often results in a public international agreement, the process necessarily involves a high level of confidentiality.

Customary practice and treaties prohibit the use of coercion against diplomats. The protection extends in varying degrees to a diplomat’s person, papers, personal property, facilities, communications, and movements. Article 29 of the Vienna Convention on Diplomatic Relations states: “The person of the diplomatic agent shall be inviolable. He shall not be liable to any form of arrest or detention. The receiving State shall treat him with due respect and shall take all appropriate steps to prevent any attack on his person, freedom or dignity.” A similar protection applies to consular posts under the Vienna Convention on Consular Relations. Furthermore, the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents, extends protection from coercion to heads of state, foreign ministers, and any
representatives of a state or international organization entitled to special protection under international law when a protected person is in a foreign state.

The nearly universal condemnation of violations against the diplomatic instrument of a state shows that a cyber attacker that steals classified cables from the US Department of State and then publishes them online to embarrass the US diplomatic corps would be in violation of international law. Such an attack would surely violate the dignity of the diplomat and his or her papers.

Each of the above is an example of a non-military action facilitated by a cyber attack. Technology permits a hostile state to act more quickly, inexpensively, and with a larger projection than in the past. Yet, the traditional governing regimes still apply. Moving coercive actions online does not mean that the actions are now unregulated; the traditional instruments that govern the economic, diplomatic, and ideological modes still apply. Hostile actions prohibited offline are equally prohibited if committed in cyberspace.

2. LOW-INTENSITY USES OF THE MILITARY INSTRUMENT IN CYBERSPACE

In many instances, despite a hostile or tense relationship, a cyber attack is not sufficiently grave for the jus ad bellum regime to govern. Low-intensity cyber attacks have consequences that are not significant enough to pass the de minimis threshold that triggers the right of a state to respond in self-defense under Article 51. While the action might be considered a prohibited use of force, the cyber attack may be insufficiently grave to warrant unilateral action. Even fewer guidelines exist insofar as a low-intensity cyber attack falls below the “use of force” threshold. But even these actions are subject to regulation through human rights law and international treaties.
Human rights law may impede states that seek to coerce others through low-intensity cyber attacks. Article 17 of the International Convention on Civil and Political Rights (ICCPR) states that “[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”Cyber attackers that gain remote-access to a user’s computer files or that falsify electronic records to besmirch an individual run afoul of this ICCPR provision.

Another problematic area of human rights law for cyber attackers is Article 19, which prohibits cyber that obstruct communication. Article 19 states that “[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.” Cyber attacks that inhibit access to the Internet or other telecommunications—such as a DDoS attack—violate Article 19. Enforcement, however, presents a significant challenge to cyber attack victims, which is a characteristic problem of human rights law. Again, the difficulties of international actors in cyberspace are not so different from the troubles of conventional international law.

How might a state respond to cyber attacks that do not trigger the right of self-defense? Does a targeted state have to absorb all low-intensity hostile actions without flinching or does international law permit a response? If a response is lawful, are there restraints on how a state may respond to low-intensity cyber attacks?

---

Even without a clear set of rules, states can and do unilaterally respond to low-intensity cyber attacks that fall short of an armed attack. Thus, this Section considers what rules ought to apply for responding to low-intensity attacks.

A state may always respond to actions that it perceives to be hostile, so the question of where a cyber attack falls on the armed attack scale is moot. Rather, the question is, how might a state lawfully respond? The answer depends on the magnitude and duration of the attack. Under international law standards, countermeasures must comply with the principles of necessity and proportionality. Accordingly, although a cyber attack may not merit self-defense, a state may nonetheless respond to it in kind.

Customary practice permits countermeasures in response to low-intensity attacks.128 Countermeasures consist of either retorsions or reprisals and they are not limited to responding to wrongs inflicted by armed force. Countermeasures often respond to both economic and political wrongs.

Retorsions are unfriendly but lawful actions. States undertake them to remedy a hostile action—like a low-intensity cyber attack—committed by an adversary. In the world of cyber attacks, such a remedial action might involve shutting off the hostile state’s access to internal servers until the targeted state feels secure that no more cyber attacks are forthcoming.

In contrast, reprisals are actions that would be otherwise unlawful, but are a justified response to an adversary’s unlawful actions. Before engaging in reprisals, a state must comply with several criteria. First, the state must be taking action in response to a wrongful

---

128 Reisman & Baker, supra note 72, at 90.
action directed against it. \textsuperscript{129} Second, the targeted state must have called upon the aggressor to discontinue his or her wrongful conduct or make reparation for it. \textsuperscript{130} Third, the effects of the countermeasure must be commensurate with the injury suffered. \textsuperscript{131} In essence, the countermeasure must consider the intention and consequences of the precipitating wrongful act.

For instance, in 2009, the United States publicly announced its intention to conduct a cyber war exercise known as Cyber Storm—to test the defense of computer networks—in collaboration with other nations including Japan and South Korea. Shortly after the announcement, the North Korea media responded by characterizing the pending exercise as a cover for an invasion. During the Fourth of July holiday, a botnet began a DDoS attack against US and South Korean government websites and international companies. Richard Clarke claims in \textit{Cyber War} that during this attack US websites were hit with as many as one million requests per second. The attack was substantial enough to bring down the Department of Treasury, Secret Service, Federal Trade Commission, and the Department of Transportation web servers for some time over the following week. \textsuperscript{132}

In such a scenario, the United States could lawfully respond with proportionate countermeasures.

\begin{flushright}
\textsuperscript{130} Id.
\textsuperscript{131} Gabcikovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, 55-56 (Sept. 25).
\end{flushright}
Retorsions would include the United States shutting down access to its servers from North Korean servers. The nature of botnets, however, makes this an unlikely scenario. Botnets often hijack computers all over the world, and shutting down access to domestic servers from all international communication is an overly broad response. Thus, the United States might turn to other methods of retorsions to remedy the attack. For example, the United States might publicly condemn North Korea for its actions.

At the same time, the United States might also undertake reprisals in response to North Korea’s cyber attack. Once the United States or South Korea determines that the DDoS attacks rise to the level of a prohibited use of force, and if demands to discontinue or provide reparation are ignored, the United States could respond in kind with its own DDoS attacks against North Korea. However, cyber reprisals have little effect in states like North Korea that are less technologically reliant than the United States.133

The ICJ has acknowledged the existence of countermeasures as a lawful right of a state, although the international community has sought to limit armed reprisals.134 In Nicaragua, the court stipulated that a state might respond with proportionate countermeasures to a prohibited use of force that does not reach the gravity of an armed attack.135

---


134 Declaration on the Inadmissibility of Intervention and Interference In the Internal Affairs of States, II(j); G.A. Res. 2625 (Declaration on Friendly Relations) (“States have a duty to refrain from acts of reprisal involving the use of force.”).

(Iran v. U.S.), 2003 I.C.J. 161, ¶ 64 et seq., Judge Simma explained that proportionate countermeasures “consist[] of defensive measures designed to eliminate the specific threat . . . at the time of the specific incidents,” thereby indicating that countermeasures are subject to the limitations of necessity and proportionality. Another consideration is whether “less grave” attacks may be accumulated for the purposes of assessing a self-defense claim. In these instances, consecutive attacks are linked in time, source, and cause. The incidents on their own are not sufficient to trigger Article 51, but the cumulative effect can transform the series of incidents into an armed attack, so that a targeted state may respond in self-defense. A response is therefore not strictly limited to the event that changed the tide, but may look retrospectively at the accumulation of activity. Thus, a large-scale response may be appropriate to a series of accumulated small-scale cyber attacks. For many, such a possibility is unsatisfying. It suggests that the United States might respond to a DDoS attack with missile strikes, if the DDoS attack can be linked to a pattern of low-level cyber attacks.

This result, however, is similar to how states respond to cross-border hit-and-run tactics of non-state actors. If each incident were considered in isolation, the target state would have little recourse. It might act in reprisal against the state if the target state could attribute responsibility. But reprisal would require a proportionate countermeasure to the incident, which might be insufficient to deter future attacks. If a state is able to accumulate the events and exercise its right of self-defense, it is permitted to respond on a larger scale in a planned and coordinated effort against its attackers. This doctrine, while controversial, has been invoked by
several states. The ICJ even implicitly acknowledged the accumulation doctrine in the *Oil Platforms* decision. It noted that “the question is whether that attack, either in itself or in combination with the rest of the ‘series of attacks’ cited by the United States can be categorized as an ‘armed attack’ on the United States justifying self-defence.”137 The court ultimately concluded that, “[e]ven taken cumulatively,” the incidents did not amount to an armed attack. Article 15 of the Draft Articles on State Responsibility assigns responsibility “when the action or omission occurs which, taken with the other actions or omissions, is sufficient to constitute the wrongful act.”138

The accumulation doctrine is noteworthy in the realm of cyberspace. There have been relatively few—if any—cyber attacks that when taken in isolation amount to an armed attack. There are many examples, however, of a series of cyber attacks that target a state. A series of cyber attacks, if accumulated, may result in the targeted state exercising its right to self-defense under Article 51. But the threshold remains high and should still depend partly on the gravity of the individual cyber attacks. For example, the Russian cyber attacks on Estonia mentioned earlier comprised a series of incidents that lasted for several weeks, causing disruption in both communication and services in the public and private sectors. If Estonia had been able to attribute the attacks to Russia, Estonia might have invoked the accumulation doctrine with respect to the relentless cyber attacks. Whether the international community would consider the

137 Case Concerning Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 64 et seq. [hereinafter Oil Platforms].
138 *State Responsibility*, *supra* note 97, art. 15.
accumulated attacks sufficient to trigger the right to respond in self-defense would depend on the magnitude and duration of the “less grave” exhibitions of cyber attacks. That test involves a high threshold that will be difficult for most victims of cyber attacks to demonstrate.

In practice, most cyber attacks fall below the threshold of an armed attack. Many even fall below the threshold of a prohibited use of force. This does not mean that states must stand by defenseless. States can, and do, respond, to coercive tactics undertaken by hostile states with countermeasures. But the responding state must first call upon the aggressor to discontinue its wrongful conduct or make reparations. The target state may respond only if the hostile state fails to comply with its request.

A state’s response to low-intensity cyber attacks is nevertheless constrained. Any countermeasure is governed by the principles of necessity and proportionality. Thus, the effects of the countermeasure must be commensurate with the injury suffered. A state may only go beyond a proportionate countermeasure if they are responding to a series of attacks. Thus, while each individual attack remains below the threshold of an armed attack, taken together the attacks constitute an armed attack. Again, this threshold remains high in international law.

3. **Covert Cyber Attacks**

Due to the sensitive nature of national security, states do not widely disseminate information regarding their cyber capabilities. Secrecy is a necessary quality for an effective cyber attack. Without secrecy, the intended target may effectively defend or prevent an attack. Thus, there is little public information on the current stockpile of cyber weapons or how they are used in practice.
What the public does know is that most cyber attacks occur covertly,\(^{139}\) where the perpetrator is an unknown actor or where the cyber attack itself is unknown. The exposed “covert” operations—such as the cyber attacks on Estonia—are publicly known due to their widespread effects on civil society or because the attack had an observable physical manifestation. There is also the possibility that information regarding a cyber attack is deliberately unveiled to deter adversaries or because the victim publicly condemns the action.

Regardless of how the public learns of a cyber attack, the scraps of available public information indicate that a vast majority of cyber attacks is committed covertly, outside the context of war. Does an action’s lawfulness change based on whether a perpetrator’s identity is concealed? How should international law govern covert cyber operations?

There are times when secrecy benefits the international public order. For one, an outcome achieved without force by a covert operation avoids escalation into a military conflict and its attendant costs.

On the other hand, the danger of covertness lies in the lack of state accountability. For example, if a state overtly seeks to stop its adversary’s nuclear weapon program, its adversary receives domestic and international public condemnation from others, who also wish to stop the nuclear weapon program. The element of transparency has two important functions for the regulation of force. First, the overt operation puts the adversary on notice of what actions it must take to cease

\[^{139}\] “Covert” in this section refers to the target’s inability to identify its attacker. While “covert” may also refer to a state operation of which its constituents are unaware, this section will refer to “covert” in the former sense. While a serious issue that deserves further scrutiny, a state that conceals its operations from its domestic audience is more closely attached to domestic law and policy concerns.
the coercive actions. Second, the architect of coercion is held accountable in an overt operation, and its actions are subject to domestic and international public and legal appraisal. Neither function is present during a covert operation.

The prohibition on the use of force under Article 2(4) does not distinguish between covert and overt attacks. If one subscribes to the textual myth of the Charter, the element of covertness does not tip the scales of justice. The Charter does not articulate tiers of unlawfulness that account for the injustice to states unable to identify what actions must take place to cease a covert attack or hold their covert attacker accountable. Under the Charter, a prohibited armed attack is unlawful whether committed covertly or overtly, and the element of covertness generally does not factor into the determination of lawfulness.

Nonetheless, the element of covertness may transform an otherwise lawful operation into an unlawful attack. There are two areas that shed light on the lawfulness of covert operations. These are the prohibition on perfidious conduct and legitimate *ruses de guerre*.

The laws of war permit a state to engage in a *ruse de guerre*. *Ruses de guerre* mislead the adversary into making a tactical mistake by catching the adversary off-guard. As articulated in Article 37 of the first Additional Protocol, a state may engage in the use of camouflage, decoys, mock operations, and misinformation, among other tactics. Secrecy and deception inhere to the effectiveness of these tactics. A cyber attack that employs a disinformation campaign by failing to secure misleading documents in military databases, such that an adversary steals false information, is a legitimate *ruse de guerre*. One of the

---

incentives to employ a cyber attack is that its covertness gives an attacker a tactical advantage. After all, an enemy possesses no right to be notified before an attack, nor does the enemy possess the right to be free from surprise attacks or ambushes.

The deceptive tactics of the attacker, however, are still constrained. Article 37 of the first Additional Protocol prohibits killing, injuring, or capturing an adversary by resort to perfidy. The provision defines perfidy as “[a]cts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence.” Among the enumerated examples of perfidy is the feigning of civilian, non-combatant status. Similarly, under Article 4 of the Third Geneva Convention, a state’s forces must “carry arms openly” and have a “fixed distinctive symbol recognizable at a distance.”

In Ex parte Quirin, a group of German soldiers during World War II removed their uniforms so that they could slip into the United States in civilian clothing. The US Supreme Court held that while the intended targets—US war facilities—were legitimate and lawful targets, it was “the absence of uniform that render[ed] [the German soldiers] liable to trial for violation of the laws of war.” Thus, the nominal element of covertness can transform an otherwise lawful operation into an unlawful

141 Id.
143 Ex parte Quirin, 317 U.S. 1, 15 n. 12 (1942).
action under international law.\textsuperscript{144} The laws of war tolerate ruses to mislead an adversary, but not to the extent of misleading an adversary of one’s status as a non-combatant.

The purpose of these provisions is to make the lawful combatants in a conflict identifiable so that a targeted state may discriminate between lawful combatants and civilians. The Commentary clarifies who are combatants and who are civilians.\textsuperscript{145} By separating combatants and civilians into separate categories, civilians are better protected and the evils of war are mitigated.

To comply with the laws of war, a state must ensure that its forces are distinguishable from the civilian population. Those laws require combatants to self-identify by means of a fixed distinctive symbol, although they do not specify what else a state’s forces must do to comply. Although a fixed distinctive symbol is often a uniform, it is possible that other symbols could comply.

In cyberspace, however, the requirement to wear a uniform does not make sense. But an identifying line of code is both possible and consistent with the intent of Article 4. However, both obligations within the Third Geneva Convention apply to the cyber attacker and not to the cyber weapon. A state could formally comply with the strict language of this provision by having its cyber attackers in uniform while safely tucked away thousands

\textsuperscript{144} State practice does not always follow this standard. In World War II, a British officer was commended for using civilian clothing to infiltrate a German base to kill a general. W. Hay Parks, \textit{Memorandum of Law: Executive Order 12333 and Assassination}, \textit{Army Law}, Dec. 1989, at 6.

of miles away from the “battlefield,” thereby reducing the distinctive symbol obligation to an empty requirement.

In practice, the operational norm is not aligned with the aspirational message of the Charter. Scholars such as W. Michael Reisman and James Baker III make the case that operations, which may be lawful if done overtly, might be unlawful if undertaken covertly.\textsuperscript{146} Thus, some covert cyber attacks would be less permissible than identical overt cyber attacks.

Factors condition the international response to covert actions. Among these are whether the covert action (1) is executed through the military instrument or another mode of coercion; (2) involves independent and disproportionate violations of other norms governing violence; (3) is governmental or non-governmental; and (4) is a single operation or integrated into an overall mission.\textsuperscript{147} Together, these factors influence whether the international community considers the covert nature of the action unlawful.

The laws of war are designed to regulate the use of force and moderate its consequences. Clear rules of how to operate on a battlefield—or in cyberspace—brings order to war and protection for noncombatants. To the extent possible, trust must exist that each participant is fighting under the same operational code. The absence of trust leads to escalating paranoia that encourages higher levels of violence and treachery, putting noncombatants at a greater risk.

Do covert cyber attacks put civilians at risk of being misidentified as the perpetrators? States have been wrongly accused of perpetrating a cyber attack, so it is conceivable that a reprisal or an act in self-defense

\textsuperscript{146} REISMAN & BAKER, \textit{supra} note 72, at 30.
\textsuperscript{147} \textit{Id.} at 67-72.
aimed at an accused state could cause civilian deaths. Further, the scenario of a targeted state misattributing an attack to civilians and taking action in violation of international law is more likely in peacetime than in conflict. During a conflict, a cyber weapon operates like any other. Though it may cross into the threshold of perfidy, the element of covertness during a conflict should not transform an otherwise lawful attack into a violation of the laws of war. In a conflict, the participants are known. If a cyber attack occurs, it is likely attributed to the adversary state rather than to a civilian group, thereby mitigating the effects on civilian life of a countermeasure. A covert cyber attack that is executed during a conflict is less likely to raise questions than one where the targeted state is not on notice of what actions it may take to cease the operation.

The situation is different during peacetime. A state is not on notice of who is attacking or what actions it can take to stop an attack. Take, for instance, an action meant to coerce a country by targeting its economy. Economic coercion is necessarily overt. Such a strategy is meant to coerce rather than destroy. By acting overtly, an actor communicates a message designed to change the behavior of the target. A covert use of the same strategy delivers no message, as the targeted state will not know the identity of the actor. Without the identity, the targeted state is bereft of strategies it might adopt to terminate the action—does the state comply with the aggressor’s demands or take countermeasures?

148 In the 1998 Solar Sunrise attacks, computers based in the United Arab Emirates breached military computers in the United States. It was later reported that it was not an attacker actually from the United Arab Emirates behind the attack, but an Israeli teenager and two high school students from California. Christopher C. Joyner & Catherine Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework, 12 EUR. J. INT’L L. 825, 839 (2001).
Otherwise lawful conduct *executed covertly* ought to be factored into the lawfulness of a cyber attack during peacetime. Although, even if the element of covertness was given more weight during peacetime, a cyber attacker could post its demands anonymously, thereby reducing the effect of covertness in determining the lawfulness of the action.

The rules of engagement in cyberspace are still emerging. During this incipient stage, adversaries continue to test the tolerance of one another and the international community. Toleration for covert actions below a certain threshold has emerged as part of the current paradigm. States endure cyber attacks without resorting to international fora when the consequences are minimal and have little effect on the balance of powers.

Legal considerations of covertness will gain greater resonance as states increasingly employ covert cyber attacks to achieve their goals. There is no bright-line rule on whether a covert cyber attack will be held unlawful by the international community for the reason of its covertness. Whether a covert cyber attack is held unlawful depends on a number of contextual factors, including: (1) who perpetrates the attack, (2) who is the target, (3) whether civilians are at risk, (4) whether the intended outcome is to coerce or to destroy, (5) whether the target is afforded an opportunity preceding the covert operation to change its offensive behavior, (5) whether the attack complies with *jus in bello* obligations, and ultimately, (6) whether the covert cyber attack complies with the fundamental policies of the Charter.

C. JUS IN BELLO: CONDUCT OF CYBER WARFARE

Once a state has entered into a conflict, the use of force is governed by *jus in bello*. Under *jus in bello*, even states that have the lawful right to use force still have limitations in how they use it. *Jus in bello* is largely
derived from the Hague Conventions, \textsuperscript{149} the Geneva Conventions, \textsuperscript{150} and the associated protocols, \textsuperscript{151} much of which is considered customary international law. In the words of the Saint Petersburg Declaration of 1868, the aim of the laws of war is to “alleviate as much as possible the calamities of war.” \textsuperscript{152} This section examines how the law of armed conflict ought to apply to cyber attacks. The restraints on how a state conducts its use of force is not contingent on the weaponry used, so transposing the principles of international humanitarian law to the use of cyber attacks—despite being a new weapon of warfare—is not only possible but also appropriate given its growing popularity as a coercive tactic. The following Sections will discuss the traditional schema of \textit{jus in bello}—military necessity, distinction,


proportionality, perfidy, and neutrality—in relation to cyber attacks.

1. **Military Necessity**

When a cyber attacker is party to a conflict, international humanitarian law restricts the use of force to targets that will accomplish valid military objectives. Considered customary international law,153 Article 52 of the Additional Protocol to the Geneva Conventions limits lawful targets to “those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”154 Notably, Article 23 of the Fourth Hague Convention forbids destruction or seizure of property “unless such destruction or seizure be imperatively demanded by the necessities of war.” Violating the principle of military necessity is considered a “war crime” in the Rome Statute of the

---


154 Protocol I, supra note 46, art. 52; see also Case No. 47, The Hostages Trial, The United States of America vs. Wilhelm List, et al., United States Military Tribunal, Nuremberg, pg. 66, (ix) The Plea of Military Necessity, http://www.ess.uwe.ac.uk/wcc/List4.htm (“Military necessity permits a belligerent, subject to the laws of war to apply any amount and kind of force to compel the complete submission of the enemy with the least possible expenditure of time, life and money.”); Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 73 (Nov. 6) (“The requirement of international law that measures taken avowedly in self-defense must have been necessary for that purpose is strict and objective, leaving no room for any “measure of discretion”).
International Criminal Court. Valid targets are thereby limited to those objects contributing to an adversary’s war efforts or those whose damage or destruction creates a definite military advantage.

A cyber attack that targets an adversary’s military computer systems satisfies the condition of military necessity by virtue of their exclusive military association. There great opportunity to attack the computer systems of a modern military. Modern militaries use computer systems for every facet of operations.

But determining whether a target creates a “definite military advantage” is complicated. Presumably, this requirement limits cyber attacks with indeterminate military advantages. The complexity of computer systems makes calculating military advantage a challenge. The value of a cyber weapon often lies in its cascade effect on systems that rely upon the initial target. Most cyber attackers do not have sufficient information to predict the indirect effects of an attack. A cyber attacker that penetrates into the computer systems of an electrical generator might gain a military advantage, but the system may have unforeseen layers that prevent such an advantage from occurring. In these circumstances, the military advantage is not definite enough to satisfy the condition of military necessity.

Similar to conventional warfare, the conundrum is that cyber attacks could be deemed as creating a “definite military advantage” ex post whereas an ex ante analysis of the same attack might not come to the same conclusion. The definitiveness of the military advantage ex post is apparent only if the attack is successful. A cyber attacker could defend challenges to its use of force

---

by creating an information log that records what information the attacker knew about the target system at the time of attack. While the laws of war do not require such recordkeeping, an information log would be a relatively simple way to shield the attacker’s decision to invoke military necessity to target an object.

Ultimately, the evaluation of whether a cyber attack arose from military necessity, will rely on a case-by-case determination. (This is similar to the evaluation of military necessity in traditional attacks.) In each instance, a cyber attacker must affirmatively determine that the attack offers a military advantage.

2. DISTINCTION

Military necessity is weighed against other limiting principles, including the principle of distinction. Article 48 of the Additional Protocol—considered a customary definition of distinction—requires attackers to “at all times distinguish between the civilian population and combatants, and between civilian objects and military objectives.” Article 51 of the Additional Protocol requires attackers to ensure that “the civilian population and individual civilians . . . enjoy general protection against dangers arising from military operations” and “not be the object of attack.”156 Article 51, therefore, prohibits “indiscriminate attacks.” Notably, the Rome Statute identifies the failure to distinguish between civilians and combatants as a “war crime.” The purpose of distinction is to restrict attacks to combatants and military objectives only.

156 Protocol I, supra note 46, art. 51; see also Protocol II, supra note 151, art. 13 (providing that “[t]he civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations” and also “the civilian population . . . as well as individual citizens, shall not be the object of attack”).
Civilians who directly participate in hostilities are not protected. By virtue of participating, the civilian forfeits his protected status. But non-participating civilians sometimes die in attacks, and such civilian deaths are not per se war crimes. The principle of distinction allows for some civilian death as long as state makes reasonable efforts to distinguish between combatants and civilians, and to refrain from intentional attacks on civilians and civilian targets. The difficulty with making this distinction with respect to cyber attacks is that in cyber space, there is often an undefined and fuzzy line between military and civilian targets. (See, for example, the description in Section I(A) of how ARPA used the civilian infrastructure provided by AT&T to accomplish its goals.) To determine whether cyber attacks meet the requirements of distinction, a cyber attacker must establish (i) whether the attack sufficiently distinguishes between civilian and military targets, taking into account the dual-use of most Internet infrastructure, and (ii) whether the cyber attacks are conducted indiscriminately and without regard to the civilian population.

i. Do Cyber Attacks Distinguish Between Civilian and Military Targets?

The laws of war are in place to ensure that parties to a conflict target combatants rather than civilians, and, if civilians are targeted, to ensure that such individuals have forfeited their protected status. To determine whether cyber attacks properly distinguish between civilian and military targets, one must understand where the distinction between the two lies.

Combatants consist of all organized armed forces, groups, and units that are under the command of

---

157 Protocol I, supra note 46, art. 51.
These individuals may rightfully participate in hostilities. Under the law of armed conflict, combatants are required to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack. Non-combatants are understood to be civilians and enemy personnel out of combat.

The definition of a lawful combatant under international humanitarian law requires a level of organization or state command responsibility. These traits are present within states with armed forces that have cyber capabilities. This also includes the ad hoc groups, such as the Russian Business Network, that receive implicit consent to act and, arguably, even direction from the state in their cyber attacks. The international humanitarian law definition of combatant is an awkward fit for cyberspace, where unorganized individuals can readily participate in cyber attacks against an adversary, as when hacktivists perform DDoS attacks for patriotic or ideological reasons. In those instances, should the targeted state be permitted to respond with a proportionate level of force? This is a pertinent question as cyber weapons become increasingly available to the masses.

In the realm of cyber war, hacktivists do not fall within the definition of lawful combatants and therefore are not treated as protected civilians under Protocol I “for such time as they take a direct part in hostilities.” Therefore, during the time that hacktivists participate in a conflict, they are valid targets. However, any use of force against them is limited by the principle of

---

158 Id. art. 43.
159 Id. art. 44(3).
160 Id. art. 50(1).
161 Id. arts. 47, 51 (3); see also Protocol II, supra note 151, art. 13.
proportionality. To the extent that hacktivists “carry arms openly” and are responding defensively, they could fit into the category of *levee en masse*, and receive Prisoner of War status under Article 4(a)(6) of the Third Geneva Convention, which extends protections to:

Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.

What it means to “carry arms openly” in cyberspace is undefined as of yet. The efficacies of most cyber weapons stems from their ability to allow cyber attackers to penetrate a computer system undetected and inject their attack.

Cyber attacks often come quickly and without warning. There can be a significant lag time before the targeted state determines the source of the cyber attack. Regardless of a state’s inclination to respond with force once it discovers the hacktivist source, it is prohibited from doing so if the hacktivist is no longer participating directly in the conflict. The relative ease with which civilians can participate in cyber attacks and remain undetected makes this limitation a true threat to targeted states. Such hacktivists momentarily become acceptable military targets, but they quickly return to their civilian status while remaining a potential threat. This problem can be partially addressed by shifting responsibility to states to prohibit, prevent, or stop cyber attacks from originating on their Internet infrastructure. States that do not comply would be internationally responsible. However, the level of control necessary for a state to comply with such a duty bumps up against the freedoms valued online. The proper balance of liberty in
cyberspace and national security will be at the heart of future debate over regulation of cyber attacks.162

A related concern under the principle of distinction is when a cyber attacker forces a civilian to participate in a conflict. Civilian computers cannot ordinarily be classified as military objects unless they are participating directly in military activities. Cyber attackers can hijack civilian computers to incorporate them in a botnet attack against an adversary, thus involving these computers in military activities.

Such hijacking involves two violations. First, the cyber attacker unlawfully attacks civilian computers with malware that forces the computer to respond to the cyber attacker’s command. The targeted state can then respond with a proportionate counter-attack against these hijacked computers, causing collateral damage to civilian infrastructure. In this case, the original cyber attacker is responsible for the subsequent damage to the civilian property caused by the targeted state. Second, the cyber attacker unlawfully forces civilians to participate in hostilities. Under the Fourth Geneva Convention, protected persons may be compelled to do

162 See, e.g., Jim Garamone, Lynn Seeks Australian Cooperation in Cybersecurity, AM. FORCES PRESS SERV. (Feb. 13, 2010) http://www.defense.gov/news/newsarticle.aspx?id=57951 (“We have the same tension you do between how do we balance between protecting this incredibly important national asset and protecting peoples’ civil liberties and the right not to face governmental intrusion . . . We’re still working through ways to balance that”); see also Cybersecurity Discussion with General Keith B. Alexander, CTR. FOR STRATEGIC & INT’L STUDIES (June 3, 2010), http://csis.org/event/cybersecurity-discussion-general-keith-b-alexander-director-national-security-agency (“We want to protect - some say the Constitution is not a suicide pact, and I agree, but it’s also not something that we’re just going to throw out our civil liberties and privacy. We were built on that. That’s how our country was built. We want to ensure that we do our part to it. My responsibility, as the director of NSA, is to ensure that what we do comports with law.”).
only work “which is not directly related to the conduct of military operations.” 163 By creating a cyber weapon composed of civilian computers, a cyber attacker unlawfully forces civilians to participate in direct military operations. This is the cyber equivalent of a “human shield.” DDoS attacks and social engineering tactics that involve civilians are questionable tactics that deserve exacting scrutiny to determine whether they violate international law principles.

Further, as previously suggested, distinguishing between civilian and military objects is complicated in cyber war.164 Targeting purely military objects will not violate the principle of distinction. However, there are cyber attacks that deliberately target objects to kill civilians or destroy civilian objects. Such attacks are clearly unlawful under the law of armed conflict. In practice, however, cyber attacks targeting civilians have been more of an inconvenience than a threat to life or safety. For instance, in 2008, tensions arose between Georgia and Russia over the separatist regions of Abkhazia and South Ossetia. The conflict escalated into war in August of 2008. Along with kinetic attacks, cyber attackers operated from Russia. Massive DDoS attacks targeted Georgia’s political websites using psychological warfare tactics, such as placing images of Adolf Hitler alongside pictures of the Georgian President. Hacktivists targeted media outlets and government websites during times of physical attacks, making communication particularly difficult and chaotic. Cyber attackers


164 Protocol I, supra note 46, art. 52.
targeted CNN and BBC web servers in Georgia, blocking access to international news as well. The attack on the media caused confusion. For the majority, however, the cyber attacks were only a temporary inconvenience. If the attacks had threatened the safety of civilians or damaged civilian property, they would have been unlawful.

A harder determination to make is whether it is unlawful to attack dual-use objects that serve both civilian and military purposes. Cyber attackers may categorize a variety of dual-use objects, such as civilian infrastructure, as legitimate military targets to the extent that they are employed for military purposes. This category includes power-generating stations, telecommunications, and bridges, among other civilian infrastructure used by the military during wartime.

In the realm of cyberspace, most Internet infrastructure can serve as a dual-use object because military systems are so often interwoven with civilian infrastructure. The US military’s global communications backbone consists of seven million computing devices on thousands of networks across hundreds of

---

installations in dozens of countries. One study approximates that ninety-five percent of the telecommunications of the Department of Defense travels through the Public Switched Network. Private investment in the underlying infrastructure of the Internet was a key factor in its worldwide spread. Unfortunately, the inter-connected nature of military and civilian infrastructure complicates the lawfulness of cyber attacks by making much of the Internet a dual-use object.

The decision to employ cyber attacks when targeting dual-use objects necessarily hinges on the intent of the attack. A cyber attacker may lawfully target a dual-use object when the purpose of the attack is to gain a military advantage. Contrast this with an attack whose purpose is to demoralize the populace. In the latter case, the attacker is not acting lawfully because the primary object of the attack is not to undermine the military but to undermine civilians’ political support for the conflict.

\textit{ii. Are Cyber Attacks Conducted Indiscriminately?}

Even if a cyber attack properly distinguishes between a civilian and combatant, a cyber attacker must ensure that its attack operates discriminately to comply with the civilian/combatant distinction. Indiscriminate attacks are those that are so imprecise as to cause collateral damage. Some degree of collateral damage is expected in wartime. After all, war is messy. The


The proportionality requirement is an attempt to limit states from engaging in a foreseeably excessive level of force by requiring states to use lesser methods of force that reduce unnecessary collateral damage when possible.

Article 57 of Additional Protocol I declares that, “when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.”\textsuperscript{168} Customary law as reflected in Article 57 of the Additional Protocol requires attackers to take “constant care” and “all reasonable precautions” to spare the civilian population and civilian objects. The Additional Protocol, Article 51(4) defines three types of indiscriminate attacks, including attacks that: (1) “are not directed against a specific military objective,” (2) “cannot be directed at a specific military objective,” and (3) “cannot be limited as required by [international humanitarian law].”\textsuperscript{169}

As the definition implies, restraint and control are necessary traits to satisfy the requirement of discrimination. Ideally, cyber weapons would be designed in a manner that permits their operation only against military objects. But this is not always possible. Therefore, the limiting principle is that the more narrowly designed the cyber weapon is to achieve its intended objective, the more likely it is to meet the requirements of discrimination. Importantly, the restraints in international humanitarian law are not meant to be a suicide pact. A state that possesses the ability to design a narrowly tailored cyber weapon is not required to use it if the implementation will endanger its own forces. A state that believes a cyber attack has a thirty percent chance of success in taking down an adversary’s

\textsuperscript{168} Protocol I, \textit{supra} note 46, art. 57(3).
\textsuperscript{169} \textit{Id.} art. 51(4).
radar system might choose to engage in a kinetic aerial bombardment with a higher rate of success to avoid risking the lives of their own soldiers.

All things being equal, in many instances, a cyber attack is preferable to a kinetic attack. A cyber attack that takes down an electrical generator will have less physical damage and fewer civilian deaths than a comparable kinetic attack from an aerial bomber. The ability of a cyber attack to disable an adversary’s systems without an explosion is inherently more discriminating than a kinetic attack that destroys the same system but also kills the technician operating the system.

But the relative inability of a cyber attack to discriminate raises questions of its lawfulness. Military systems are usually more secure than civilian systems. Therefore, it is easier to unleash a cyber attack that targets a civilian system on which the military relies rather than to attack the military system directly. Further, predicting and understanding the outcome of a cyber attack requires a substantial amount of intelligence on the systems targeted. Even with this information, the number of factors outside of a cyber attacker’s control can mean that a cyber attack unintentionally spreads beyond the intended target. Cyber attacks that employ a virus or a worm, for example, can quickly spiral out of control, infiltrating civilian systems and causing damage to property that far surpasses the intent of the cyber attacker.

One example of a cyber attack designed to distinguish between a civilian and a military object with the intent of attacking discriminatingly is the Stuxnet worm that targeted nuclear facilities in Iran. Stuxnet, a sophisticated computer worm designed to attack industrial control systems, appeared in the cyber
ecosystem in 2010. The worm had two main components. One was designed to force Iran’s centrifuges to spin out of control. The other was to deceive operators into thinking the machines were operating normally when they were actually tearing themselves apart. The level of sophistication was unprecedented. Not only was Stuxnet designed to upload information about the system it infected to a command-and-control server so that attackers could pick their targets and change how they physically operate, it also appears that it was designed to trigger its payload only for the Iranian nuclear program.

Stuxnet targeted computers known as controllers, which run industrial machinery. These controllers are critical to the successful operation of the uranium enrichment facilities necessary for a nuclear program. The Stuxnet worm became operational when it detected a specific configuration of controllers running a particular set of processes found only in an enrichment plant. While the Stuxnet worm infected civilian industrial control systems around the world, its harmful effect operated directly and exclusively on specific systems and conditions present in Iran’s nuclear

---

program. The Stuxnet worm satisfies the criteria of distinction because the worm was designed for a specific military target—assuming the Natanz plant is not a civilian nuclear energy program—and did not indiscriminately destroy civilian computer systems.\footnote{Yaakov Katz, \textit{supra} note 171.}

Distinction is a problem for cyber attackers, whose targets are very frequently dual-use. However, if the intent of a cyber attack is to achieve a military advantage by targeting computer systems used for military objectives, and if the attackers conduct such attacks with reasonable precaution for likely collateral effects, cyber weapons are a more precise and adaptable means for attack than traditional weapons.

3. \textit{Proportionality}

The principle of proportionality is similar to distinction in that it reflects concern with the consequences of an attack on civilians and civilian objects. Proportionality governs the degree and kind of force used to achieve a military objective by comparing the expected military advantage gained to the expected incidental damage caused to civilians and civilian objects. As one court notes, the laws of war “create\[] a delicate balance between two poles: military necessity on one hand, and humanitarian considerations on the other.”\footnote{HCJ 2056/04 Beit Sourik Village Council v. The Government of Israel [2004], art. 34 (Barak, C.J.), http://elyon1.court.gov.il/files_eng/04/560/020/A28/04020560.a28.htm (quoting Dinstein, \textit{Legislative Authority in the Administered Territories}, 2 iyunei Mishpat 505, 509 (1973)).}

The principle of proportionality stems from Article 51 of Additional Protocol I, which states that force is prohibited where it “may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which
would be excessive in relation to the concrete and direct military advantage anticipated.” Article 57 similarly requires that attackers “refrain from deciding to launch an attack which may be expected to cause incidental . . . [but] excessive [losses] . . . in relation to the concrete and direct military advantage anticipated.” The Rome Statute incorporates proportionality within its enumeration of particular crimes. Article 8(2)(a)(iv) references “extensive destruction . . . not justified by military necessity” and Article 8(2)(b)(iv) states that “intentionally launching an attack in the knowledge that such attack will cause incidental loss . . . or damage . . . would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.” In Beit Sourik, the court articulated the principle as focusing on “the relationship between the objective whose achievement is being attempted, and the means used to achieve it.”

An attack that results in civilian deaths or destruction to civilian property is not a per se violation. What is prohibited under the principle of proportionality is an attack that is reckless, or an attack that knowingly takes civilian lives or destroys civilian property in excess of what is necessary for accomplishing a military objective. That is not to say that there is only one appropriate means to achieve an end. Courts have

173 Protocol I, supra note 46, art. 51(5).
174 Beit Sourik, supra note 172; see also Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, 147 (Dec. 19) (“The Court cannot fail to observe, however, that the taking of airports and towns many hundreds of kilometers from Uganda’s border would not seem proportionate to the series of transborder attacks it claimed had given rise to the right of self-defence, not to be necessary to that end.”).
recognized that there may be a zone of proportionality within which a commander has discretion to act.\textsuperscript{175}

Proportionality applies to the indirect effects of an attack as well. For instance, a cyber attack is responsible for the indirect effects on a civilian population caused by an attack on the control system of an electrical generator. Some attacks have such dangerous indirect effects that they are prohibited outright. As stated in Article 56 of Additional Protocol I, “works or installations containing dangerous forces, namely dams, dykes, and nuclear electrical generating stations, shall not be the object of an attack, even where those objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.”

The principle of proportionality ought to make attackers prefer a cyber attack to a kinetic attack. One of the benefits of a cyber attack is that it permits a state to minimize collateral damage. As previously noted, a cyber attack will usually be less deadly than a kinetic attack. Additionally, a cyber attack is potentially reversible. These traits are desirable for a state that wants to apply a level of proportionate force without causing a disproportionate number of civilian casualties.

There are challenges, of course, to whether a cyber attack can meet the necessary requirements to be considered lawful. For example, without a mechanism to reverse an attack, cyber attacks do not allow a target to surrender. Unlike an attack that uses a human operator who can assess changed conditions, a cyber attack that is unleashed into the cyber environment without the ability

\textsuperscript{175} Beit Sourik, \textit{supra} note 172; see also Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, 50 (2003) (referring to the principle of proportionality in warfare, the committee “suggested that the determination of relative values must be that of the “reasonable military commander”).
for recall cannot take into account a targeted state’s desire to surrender—a customary right under international law.

As cyber attacks grow increasingly sophisticated, cyber attackers will be able to control them better. For instance, Stuxnet incorporated features designed to limit its effect. Rather than unleash a worm that caused malfunction in all the machines that it infected, Stuxnet operated on a specific target. The destructive effect self-activated only when it encountered the conditions present in that specific target. Stuxnet was also designed to self-destruct when its lifecycle expired in 2012. Features like these better ensure that a cyber attack’s effects are limited and proportionate to the military advantage that the attackers hope to gain.

Cyber attackers are not well positioned to refute claims of indirect collateral damage. This presents a problem when a targeted state brings a claim against a cyber attacker. A targeted state has an incentive to exaggerate the effects of force when presenting the attack to its populace and arguing for recourse before the international community. Disproving a state’s claim that it experienced inordinate indirect effects from a cyber attack would be difficult. To overcome this problem, the burden of proof should remain with the targeted state. This also reduces the incentive for a state to bring unsubstantiated claims against the cyber attacker. Thus, a state that alleges a war crime would need to bring evidence that a cyber attack was the cause of a disproportionate amount of civilian property damage or death.

The proportionality analysis of a cyber attack must always be considered on a case-by-case basis. A formula that compares the number of civilians killed to the number of combatants killed is insufficient. Rather,
one must consider the value of the target and whether the
attack offered a definite military advantage and showed
proper caution vis-à-vis civilian life and property.

4. Perfidy

The prohibition on perfidious conduct arises from the
desire to restore peace without completely
destroying one’s adversary. Perfidy is a form of
deception, in which one side insists that it is acting in
good faith in conducting hostilities but, once an
opportunity presents itself, deliberately acts in bad faith.
Such unlawful conduct is prohibited under Additional
Protocol I, which states that “[a]cts inviting the
confidence of an adversary to lead him to believe that he
is entitled to, or is obliged to accord, protection under
the rules of international law in armed conflict, with
intent to betray that confidence, shall constitute
perfidy.”176 Perfidious conduct is prohibited under the
law of armed conflict because it undermines the ability
to restore peace.

One example of prohibited perfidious conduct is
if an adversary fires upon armed forces that have already
raised the flag of surrender. Raising the flag of surrender
carries the implicit promise to lay down arms. Under the
prohibition on perfidy, firing in this circumstance is
prohibited because using adherence to the law of armed
conflict against an enemy is unlawful.

Cyber warfare is enticing for those who wish to
indulge in perfidious conduct. Cyber attackers will find
bountiful opportunities to influence or mislead
adversaries because most sophisticated cyber attacks
involve some level of concealment. However,
concealment alone does not always present a violation of
lawfulness. A ruse de guerre is a common tactic of

176 Protocol I, supra note 46, art. 37; see also Hague IV, supra
note 149, art. 23(b) (“to kill or wound treacherously individuals
belonging to the hostile nation or army” is forbidden).
conventional warfare. Actions such as surprise attacks, feigning attacks or retreats, and psychological tactics are all condoned as lawful efforts to influence or mislead an enemy.

Richard Clarke, Special Advisor to the President on Cybersecurity during the Bush administration, wrote in *Cyber War* of an American cyber attack employed in Iraq.\(^ {177}\) Just before the 2003 US invasion of Iraq, the United States hacked into the Iraqi Defense Ministry’s E-mail system. In Clarke’s account, the Iraqi military learned that their secret “closed-loop” private military network was compromised when US Central Command (CENTCOM) sent Iraqi military officers an E-mail.\(^ {178}\) CENTCOM stated in the E-mail that the US goal was only to displace Saddam Hussein and his sons from power and they had no interest in harming their forces. The E-mail promised that, if necessary, they would overwhelm any Iraqi opposition as they had done in the Gulf War in the 1990s. Not surprisingly, many Iraqi military officials followed CENTCOM’s advice and chose to walk away from the battle before it even began.

CENTCOM’s ruse is an example of a legitimate cyber *ruse de guerre*. However, not all cyber attacks will qualify as such. For instance, a cyber attack would violate the law of armed conflict if it sent false information deceiving an adversary’s forces into believing that the hostilities are over, inducing them to lay down their arms before a ground attack.

Cyber warfare presents additional complexities in that cyber attacks can deceive targeted states into believing an attack originated from another source, whether the source is a non-combatant or a third party. Under Article 37(1)(c) of the Additional Protocol, “the feigning of civilian, non-combatant status,” is an

\(^{177}\) Hague IV, *supra* note 149.

\(^{178}\) *Id.* art. 23(b).
example of prohibited perfidious conduct. Cyber attackers that trick adversaries into thinking the attack originated from a non-combatant or a civilian violate the laws of war.

But this provision applies only to actions directed against adversaries in armed conflict; thus, an action that tricks third parties to act against adversaries remains a grey area. Such cyber attacks occurred during the Russia-Georgia conflict. There, Russian hacktivists directed their botnets to send a barrage of traffic to the international banking community, pretending to be cyber attacks originating in Georgia. The international banks responded by automatically shutting down access to the Georgian banking sector.179

The cyber attack against Georgia reveals the potential for a much larger threat. Had the hacktivists aimed their attacks at another state in tension with Georgia, they could have instigated the opening of another front in Russia’s war on Georgia. Such covert action would be perfidious, yet the law of armed conflict falls short of explicitly prohibiting such conduct.

---

Cyber attackers benefit from the failure of targeted states to detect or attribute cyber attacks. Sophisticated cyber attackers are able to operate in ways that make tracing attacks impossible. This is especially true if tracing an attack requires the cooperation of states with strong domestic privacy laws. The result is that military commanders face less accountability and have more incentives to use cyber weapons.

Perfidious conduct is reprehensible under international law because it punishes adversaries for following the laws of war, so concealing a cyber weapon alone during an armed conflict will not violate the prohibition on perfidy. But a cyber attack that employs an adversary’s adherence to international humanitarian law against the adversary is in violation of the prohibition on perfidy.

5. **Neutrality**

The principle of neutrality permits a state to declare itself neutral to a conflict and thereby protects it from attack or trespass by belligerents. Neutral states remain protected as long as they do not militarily participate or contribute to belligerent states or allow their territory to be used for such militaristic purposes.\(^{180}\) Notwithstanding these restrictions, a neutral state may maintain its relations with belligerents during hostilities.

The principle of neutrality is derived primarily from the Hague Conventions. The Hague Conventions outline (1) the rights of neutral states and their obligation not to participate in the conflict, and (2) the obligation of belligerents to respect the inviolability of neutral states.\(^{181}\) Cyber attacks jeopardize these distinct elements of neutrality. The question for cyber attackers is how the

---


\(^{181}\) Id. art. 1.
principle of neutrality applies—and whether it is relevant—in the area of cyber warfare.

Under the first clause—the neutral state’s obligation—the neutral state is prohibited from participating militarily in a conflict. To retain the title of neutrality, a state may not allow belligerents to move troops, munitions of war, or supplies through neutral territory. If a neutral state permits its territory to be used for these purposes, it loses its veil of neutrality and transforms into a legitimate target.

There is one exception to the inviolability of a neutral state’s territory. Under Article 8, a nation need not “forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals” as long as the neutral states permits the use of its telecommunications infrastructure impartially.182 Whether this exception applies to Internet infrastructure has not yet been tested.

An element of cyber attacks suggests that this exception should not apply in the domain of cyber warfare. Under the Hague Conventions, belligerents “are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power.”183 Cyber attacks operate as weapons. They are capable of causing as much damage and destruction as kinetic weapons. When malware or a DDoS attack is routed through a neutral state, this provision ought to be implicated. If one conceives of cyber weapons as munitions of war, a state’s claim of neutrality relies upon whether a cyber attack is transmitted through its Internet infrastructure.

Under the second clause—the belligerent’s obligation to the neutral state—the belligerent must

---

182 Id. art. 8.
183 Id. art. 2.
respect the inviolability of the neutral state. The perfidious use of cyber weaponry can make this requirement a challenge. A belligerent may not believe a state’s claim to neutrality if a cyber attack is designed to appear as if it originated from that state. The danger lies in that a neutral state attacked for this reason may lawfully respond in self-defense, thereby broadening the conflict and violence.

What are the obligations of a neutral state when it comes to cyber warfare? It is unrealistic to require the neutral state to prevent a cyber attack from originating in its territory because of the complex Internet infrastructure involved in perpetrating, as well as preventing, a cyber attack. Cyber battlefields do not exist in a concentrated area. The Internet infrastructure is disparate and extends globally. The method of “distributed communications” developed by Paul Baran and incorporated into the packet switching foundation of the Internet ensures that no user can realistically predict what route information, legitimate or malicious, will take to reach its destination. Information will take whatever is the shortest route to its destination depending upon the real-time conditions at each node. The inability to predict what route malware will take to reach its destination combined with a duty to prevent facilitating an attack would require a neutral state to sever all of its Internet connections in order to remain neutral. Otherwise, a neutral state may unwittingly transmit a cyber attack either directly to the belligerent state or indirectly by routing through another “neutral” state. Such a requirement is impractical.

Neutral states ought to have a way to maintain their neutrality without being held to unrealistic limitations. One commentator suggests viewing the duty of a neutral state through the framework of the law of naval warfare. Under naval warfare, the test to evaluate a
neutral party is the “means at its disposal.” 184 Thus, a neutral state would need only use the means at its disposal to detect and repel a belligerent’s cyber attack within its jurisdiction. Another option is to adopt an intent-based view of neutrality. Under this view, a belligerent does not violate the principle of neutrality unless it intentionally directs cyber weapons through the Internet nodes of a neutral state. Similarly, a neutral state would not be held responsible for unintentionally allowing a cyber-weapon to pass through its jurisdiction. A state put on notice of an ongoing attack ought to cooperate to cease the attacks or else be held complicit.

It is important to maintain the principle of neutrality to prevent warfare from spreading. The infrastructure of the Internet presents practical problems for a state attempting to be neutral under the current international humanitarian law framework. A re-interpretation of neutrality that permits a state to maintain its neutrality despite its cyberspace infrastructure “facilitating” attacks is necessary to preserve the spirit of neutrality. A state ought to be able to maintain its neutrality as long as it upholds its duty “not to allow knowingly its territory to be used for acts contrary to the rights of other states.”

6. Unnecessary Suffering

The prohibition against unnecessary suffering restricts a state’s arsenal by prohibiting certain types of weapons. International humanitarian law recognizes that “[t]he rights of belligerents to adopt means of injuring the enemy is not unlimited.” 185 As noted in an ICJ advisory opinion on nuclear weapons, “states do not have unlimited freedom of choice of means in the

184 Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, art. 8, entered into force Oct. 18, 1907.
185 Hague IV, supra note 149, at art. 22
weapons they use." The ICJ based its finding on the principle that, “[I]t is prohibited to cause unnecessary suffering to combatants: it is accordingly prohibited to use weapons causing them such harm or uselessly aggravating their suffering.”

This prohibition encourages states to use the appropriate level of force to achieve their military ends. The basic idea is that harm should be no greater than is necessary to achieve legitimate military objectives. Under this principle, indiscriminate weapons, such as biological or chemical weapons, are unlawful.

The prohibition on unnecessary suffering cuts both ways in the realm of cyber warfare. On one hand, cyber attacks are often difficult to control, and thus, indiscriminate in their effects. A cyber weapon that employs the use of a worm can unintentionally infect millions of computers in its efforts to act on a single targeted network. Further, a discrete cyber attack can cause unnecessary suffering because it does not arouse suspicion and therefore leads to excessive harm. Consider, for instance, a cyber attack that targets the medical records of an enemy’s military commander. If the military commander is given improper treatment that causes unnecessary suffering, the cyber attacker arguably violates the principle against unnecessary suffering. Yet cyber weapons often present the lowest level of force that can be employed when compared with a traditional kinetic attack. A kinetic attack that bombs a building in order to shut down an electrical generator will result in more damage and destruction than a cyber attack targeted at the same electrical generator. Thus, military commanders will often find it preferable to use

---

186 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257 (July 8).
187 Id.
a cyber attack because it may spare lives and physical infrastructure.

Whether a cyber weapon violates the prohibition on unnecessary suffering is often a case-by-case determination that examines all relevant factors. A good rule of thumb is that a cyber attack is unlawful if its consequences are similar to a kinetic attack that violates the prohibition on unnecessary suffering.

III. CONCLUSION

Cyber attacks are here to stay. Cyber attacks provide a low-cost, remote, instantaneous, and powerful tactic of coercion or destruction, often without triggering accountability. These attributes guarantee that states and non-state actors will continue to develop and unleash cyber attacks in the foreseeable future.

This Article examined to what extent this new form of hostile behavior can be regulated under the existing regime of the laws of war. This Article considered how cyber attacks work, how they are being used in practice, and in what manner international humanitarian law relates to the use of cyber weapons. Without governance—and constraints—from international law, cyberspace will remain a relatively lawless battleground.

Many difficult questions arise when trying to fit cyberspace within a warfare regime constructed long before even the most visionary policy makers imagined cyber weapons. But the problems generated by cyber attacks are often similar to the problems of conventional attacks. The differences between conventional and cyber warfare are of degree, not of kind. Thus, the international humanitarian law regime governing conventional warfare can be effectively transposed to cyber attacks.

Cyber attacks present a litmus test for a nation’s commitment to international law. The problem of
attribution in cyberspace means that cyber attackers have the capability of coercion on a state without the resultant responsibility. Therefore, the cyber attacker may experience great temptation to violate principles and obligations of international law to achieve the attacker’s ends. This threat has generated a substantial amount of interest in rethinking cyber security. While some experts have advocated for less online anonymity and more government control over the cyberspace infrastructure, other solutions exist that create fewer domestic liberty concerns.

The impetus that sparked the innovation of the Internet was the concern of the United States to build a survivable communications system. Today, states experience the same need to create resiliency in their cyberspace infrastructure. Responding to the threat of cyber attacks lies as much in the area of mitigation as it does in the area of attribution. Mitigation means creating systems of redundancy (colloquially known as back-ups) to ensure that systems stay online. Mitigation also means deploying greater intelligence to listen in on chatter of impending cyber attacks so that a state may properly preempt or prepare.

Whatever policies a nation implements to defend its cyberspace infrastructure from attackers, international law must play a role to deter unlawful action by making offenders accountable to international appraisal. An international treaty that regulates the rules of engagement online would certainly be a helpful addition to the corpus of the laws of war. However, in the current international climate, such an addition to the laws of international war is unlikely in the near future. Fortunately, the lack of a cyber-war addendum to the laws of war does not mean that cyber attacks are unregulated. States may continue to rely on the existing regime of international law to regulate cyber attacks,
while they await the international community’s response to this modern form of waging battle.
If You Wish Cyber Peace, Prepare for Cyber War:
The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare

By Michael Preciado*

I. INTRODUCTION

This article will demonstrate four key points. First, that militaries around the world have implemented cyber warfare as part their military doctrines. Second, cyber warfare poses a serious threat to critical

* Michael Preciado is a 2013 J.D. Candidate of Chapman University School of Law. The author would like to gratefully acknowledge his wife, Mona Preciado, and his family for their support and encouragement throughout the writing process.

1 See Brenner, infra note 266, at 401 (cyber warfare is the conduct of military operations by virtual means).

2 See infra Part I-C (discussing the rise of cyber attacks in modern warfare); see also McAfee, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 5 (2011) (over 120 nations have or are currently developing cyber warfare capabilities).
infrastructure in the United States. Third, cyber warfare cannot be policed through international treaties. Fourth, for the foregoing reasons, the federal government needs to protect critical infrastructures in the United States from cyber warfare.

Technology, although created for the advancement of mankind, is eventually turned into a weapon of war. The Internet is no exception.

---

3 See infra Part II (discussing the dangers that cyber attacks pose to critical infrastructures in the United States); see also McAfee, In the Dark: Crucial Industries Confront Cyber Attacks 6 (2011) (85% of critical infrastructures have reported being the victims of cyber intrusions). "Exploiting vulnerabilities in cyber infrastructure will be part of any future conflict. If opponents can access a system to steal information, they can also leave something behind that they can trigger in the even of a conflict or crisis. Porous information systems have allowed opponents to map our vulnerabilities and plan their attacks. Depriving Americans of electricity, communications, and financial services may not be enough to provide the margin of victory in a conflict, but it could damage our ability to respond and our will to resist. We should expect that exploiting vulnerabilities in cyber infrastructure will be part of any future conflict." The 44th Presidency, infra note 131, at 13.

4 See infra Part III (discussing how international law, such as the United Nations Charter, will not provide an adequate legal framework to govern cyber warfare); C.f. Stuart S. Malawer, Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance, 58 Virginia Lawyer 28, 30 (2010) (international law will provide hallow results and prove to be an illusion of safety).

5 See infra Part IV (concluding that the federal government can monitor critical infrastructure in the United States through a warrant type system that protects civil liberties).

6 Ahmad Kamal, The Law of Cyber-Space: An Invitation to the Table of Negotiations 76 (2005). "Industrialization led to attrition warfare by massive armies in World War I. Mechanization led to maneuver predominated by tanks in World War II. The information revolution implies the rise of a new mode of warfare in which neither mass nor mobility will decide outcomes; instead, the side that has greater technological knowledge will enjoy decisive advantages." Id.
Throughout modern history, parties have learned how to take advantage of the Internet and how to exploit it. Initially, hackers used cyberspace to explore system networks. Criminals then learned how to use the Internet to commit personal identity theft. Similarly, terrorists learned how to use the Internet to disseminate propaganda. In the end, militaries around the world have learned how to use cyberspace for intelligence gathering, covert operations, and warfare.

As a result of nations resorting to cyber warfare, the militarized use of cyberspace poses serious dangers to the United States’ critical infrastructure. Cyber attacks have been able to infiltrate nuclear power plants and affect the power grids. Cyber attacks can

See McAfee, Virtual Criminology Report 2009, Virtually Here: The Age of Cyber Warfare 3 (2009) (nations are building up their cyber attack capabilities in what has been described as a “Cyber Cold War”).

See e.g., Krebs, infra note 61 (one of the first computer viruses, “The Brain,” was created in 1986).

infra Part I-C.

Id.

Id.

Id.

See infra Part II; see also U.S. Dep’t of Homeland Sec., Presentation, National Cyber Exercise: Cyber Storm, New York City Metro ISSA Meeting 11 (June 21, 2006) (operation Cyber Storm was a simulated attack against critical infrastructures in the United States that demonstrated vulnerabilities in the electric grids, FAA computer systems, and commuter train systems); Anthony H. Cordesman & Justin G. Cordesman, Cyber-Threats, Information Warfare, and Critical Infrastructure Protection 2 (2002) (cyber attacks threaten the United States, because information systems are becoming a major part of critical infrastructure and government). The threat of a cyber war has grown so much that some analyst predict a looming cyber “Pear Harbor.” Id.

See Schneier, infra note 139 (discussing the Stuxnet virus that allegedly corrupted Iran’s nuclear program).
theoretically crash the financial industry. Further, cyber attacks against government infrastructure have caused massive instability and confusion.

In response to the potential dangers of cyber warfare, academics have proposed that the legality of cyber warfare could be governed by analogy. Theorists have suggested that legal analogies to the Nuclear Nonproliferation Treaty, the United Nations Charter, the Outer Space Treaty, or the Antarctic Treaty System provide adequate models to govern cyber warfare. Hypothetically, these analogies provide the principles to govern cyber warfare. In practice however, these analogies provide unworkable models to govern cyber warfare. Practicing law by analogy would not adequately police cyber warfare because attributing responsibility for cyber attacks is improbable; nations will use cyber warfare as a means to force larger militaries into asymmetric warfare; and because cyber warfare can be used to attack critical infrastructure in order to thwart an enemy’s military action. Accordingly, cyber warfare cannot be properly regulated through international means.

Because the dogs of cyber war cannot be shackled by international means, the United States needs

---

15 See McAfee, supra note 1, at 17 (only 14% of the population are completely confident the financial sector could withstand a major cyber attack).
16 See e.g., Brenner, infra note 266, at 396 (an orchestrated cyber attack could infiltrate ATMs throughout the nation, crippling the financial industry).
17 See infra Part III.
18 See Shackelford, infra note 152, at 216 (analogizing responses to cyber attacks in international law).
19 See infra Part III.
20 Id.
21 Id.
22 Id.
to protect the nation’s critical infrastructure. The federal government should institute active defense measures on critical infrastructure networks. This will entail the monitoring of critical infrastructure networks for malicious code. In order to ensure that civil liberties are protected, Congress should also pass legislation that allows Cyber Command to monitor private networks upon judicial approval.

Part I will discuss the history of the Internet and the evolution of cyberspace into its ultimate utilization in cyber warfare. Part II will explain why cyber attacks pose threats to the United States’ critical infrastructure. Part III will survey the international efforts proposed to regulate cyber warfare, why they are inadequate, and why subsequent legislation will prove ineffectual as a means to regulate cyber warfare. To conclude, Part IV will propose that the federal government needs to protect critical infrastructure in the United States. This can be implemented through legislation that allows Cyber Command to monitor private networks upon judicial approval.

II. THE INTERNET AND THE RISE OF CYBER WARFARE

A. THE ORIGINS AND STRUCTURE OF THE INTERNET

The Internet was originally created for the Department of Defense (“DOD”), but later became widely incorporated within the general public. The

---

23 See infra Part IV.
24 Id.
25 Id.
26 See Cyber Command, infra note 94.
27 See infra Part IV.
28 Id.
29 Id.
30 See e.g., Stephen Segaller, Nerds 2.0.1: A Brief History of the Internet (1998); Katie Hafner, Where Wizards Stay Up Late: The Origins Of The Internet (1998).
origin of the Internet can be dated to 1969 as an experimental project of the Advanced Research Project Agency (“ARPA”).\(^{31}\) The DOD funded the project for the purpose of building a communications network.\(^{32}\) Accordingly, ARPA developed the Advanced Research Project Agency Network ("ARPANET"):\(^{33}\) a communications medium of dedicated telephone lines.\(^{34}\) ARPANET provided a series of redundant communications between the DOD, defense contractors, and defense research universities.\(^{35}\) Subsequently, ARPANET expanded to encompass corporations, universities, and the general public.\(^{36}\) “The ARPANET came to be called the ‘DARPA Internet,’ and finally just the ‘Internet.’”\(^{37}\)

The structure of the Internet is comprised of a decentralized series of networks.\(^{38}\) “No single entity—academic, corporate, government, or non-profit—


\(^{32}\) Donna Miles, *Bush Cites DOD Internet Development in Promoting U.S. Innovation*, AMERICAN FORCES PRESS SERVICE, Feb. 6, 2003 (the DOD funded the project to improve military communications).


\(^{34}\) See Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 *Naval L. Rev.* 132, 135—36 (2005). “[N]ow internet communications travel through all available communication mediums: telephone lines, microwave relays, satellite uplinks and downlinks, fiber optic cables.” Id.

\(^{35}\) See e.g., Fred H. Cate, *Privacy in the Information Age* 9—11 (1997); Salus, *supra* note 31, at 163 (the defense research universities included the University of California Los Angeles, Stanford, University of California Santa Barbara, and the University of Utah).

\(^{36}\) Cate, *supra* note 35, at 9—10.

\(^{37}\) *Reno*, 929 F. Supp. at 831.

\(^{38}\) Cate, *supra* note 35, at 10.
administers the Internet.” 39 It was designed to be a decentralized series of communication links that could reroute a message instantaneously if one or more networks were damaged or unavailable. 40 For instance, an email sent from a user in Washington D.C. to a user in California may be diverted through several other networks and further subdivided to reach its final destination. 41 The Internet is not a single streamlined entity, but rather a “giant network which interconnects

39 Reno, 929 F. Supp. at 832.
40 Id. at 831. “This redundant system of linked computers was designed to allow vital research and communications to continue even if portions of the network were damaged, say, in war.” Id.
41 Id. “A communication sent over this redundant series of linked computers could travel and a number of routes to its destination. Thus, a message sent from a computer in Washington, D.C., to a computer in Palo Alto, California, might first be sent to a computer in Philadelphia, and then forwarded to a computer in Pittsburg, and then to Chicago, Denver, and Salt Lake City, before finally reaching Palo Alto. If the message could not travel along that path (because of military attack, simple technical malfunction, or other reason), the message would automatically (without human intervention or even knowledge) be re-routed, perhaps, from Washington, D.C. to Richmond, and then to Atlanta, New Orleans, Dallas, Albuquerque, Los Angeles, and finally to Palo Alto. This type of transmission, and re-routing, would likely occur in a matter of seconds.” Id. “Messages between computers on the Internet do not necessarily travel entirely along the same path. The Internet uses ‘packet switching’ communication protocols that allow individual messages to be subdivided into smaller ‘packets’ that are then sent independently to the destination, and are then automatically reassembled by the receiving computer.” Id.; See also Antolini-Jenkins, supra note 34, at 137; George K. Walker, Information Warfare and Neutrality, 33 VAND. J. TRANSNAT’L L. 1079, 1094—95 (2000).
innumerable smaller groups or linked computer networks. It is thus a network of networks.”

B. TYPES OF CYBER ATTACKS

In order to understand what cyber warfare is, it is important to understand what a cyber attack is. Cyber warriors have three types of cyber attacks within their arsenal: syntactic, semantic, and mixed. The weapons vary in intensity, ranging from annoyance to

42 Reno, 929 F. Supp. at 830. Because the Internet is comprised of several networks, a user must connect to an Internet Service Provider (“ISP”) to access the Internet. See Antolin-Jenkins, supra note 34, at 136 (“By connecting to the ISP, the computer becomes part of the network, and it may be utilized in the process of sending messages.”). Although the Internet is comprised of several smaller networks, the majority of Internet traffic flows through large cable lines, known as dedicated “backbones.” See Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat To National Security And What To Do About It 281 (2010) (Internet backbones are comprised of national fiber optic cables operated by large Tier 1 Internet Service Providers). Maintained by large telecommunications companies, these backbones, fiber optic cables, facilitate the transmission of large amounts of data simultaneously to various regions. See Ellen S. Cohen, Broadband Internet: Access, Regulation And Policy 10 (2007) (AT&T, Verizon, Sprint-Nextel, Level3, and Quest are all Tier 1 service providers that own “backbone” cables). The backbones are then connected internationally to Network Access Points (“NAPs”). Antolin-Jenkins, supra note 34, at 136. The NAPs are the gateways through which international Internet traffic flows: “each individual entity, whether a government entity, a communications company, or a corporation with a large intranet, agrees to intercommunicate with one another through the NAPs.” Id.

43 Some theorists have classified electromagnetic weapons as cyber weapons. See Natasha Solce, The Battlefield of Cyberspace: The Inevitable New Military Branch–The Cyber Force, 18 ALB. L.J. SCI. & TECH. 293, 305 (2008). An electromagnetic weapon is used to “overload computer circuitry with a blast of electromagnetic energy.” Id. Although electromagnetic weapons can affect computer-based systems, realistically they are kinetic weapons used to short circuit electrical systems. Accordingly, they are not included in this article’s definition of cyber weapons.
devastation, but all pose serious threats to national security.

The first kind of cyber attack is the syntactic attack, a cyber attack comprised of malicious code. Malicious code is computer language designed to affect a computer’s operating system in order to modify it, retrieve information, or destroy it. Examples include viruses, worms, Trojan horses, denial-of-service (“DOS”) attacks, and distributed-denial-of-service

---

44 See Jeffrey Carr, Cyber Warfare: Mapping the Cyber Underworld 1—12 (Mike Loukides, 1st ed. 2010).
46 Antolin-Jenkins, supra note 34, at 139.
(“DDOS”) attacks. \(^{48}\) Above all, DOS and DDOS attacks are of the most concern. \(^{49}\) DOS attacks temporarily or permanently incapacitate a website by overwhelming it with false data requests. \(^{50}\) The network becomes so overworked that it crashes. \(^{51}\) DDOS attacks are similar to DOS attacks, but use thousands of botnet \(^{52}\) computers

\(^{48}\) See Antolin-Jenkins, supra note 34, at 138—140 (discussing syntactic attacks). Viruses are activated when the user opens a file. They “corrupt and destroy files in the infected computer, making the computer inoperative.” \(\text{Id.}\) at 139. “Worms replicate in the system without infecting the host computer.” \(\text{Id.}\) “At a certain point, there is so much duplication of messages, the system as a whole suffers at the least, a slow-down, and at worst, a crash of host systems overwhelmed by the traffic, thereby denying legitimate traffic a means of transportation.” \(\text{Id.}\) A Trojan horse is an executable code that upon being activated, will perform certain functions that it was created to do e.g., providing the sender of the code remote access to the infected computer. \(\text{Id.}\) In a denial-of-service attack, attackers attempt to cause computer networks to crash to prevent the public from accessing information. \(\text{See Understanding Denial-of-Service Attacks},\) US-CERT: UNITED STATES COMPUTER EMERGENCY READINESS TEAM, available at http://www.us-cert.gov/cas/tips/ST04-015.html. A distributed denial-of-service attack is distributed because the attacker uses multiple computers to launch a denial-of-service attack. \(\text{Id.}\)


\(^{50}\) Wolfgang McGavran, Intended Consequences: Regulating Cyber Attacks, 12 TUL. J. TECH. & INTELL. PROP. 259, 262—63 (2009).

\(^{51}\) Chandler, supra note 49, at 236 (discussing the effects of DDOS attacks, which are similar to DOS attacks).

\(^{52}\) “An example of a mixed weapon is a ‘bot network’ or ‘bot herd,’ which is a group of ‘bots.’ Bots are remote-controlled or semi-autonomous computer programs that infect computers. The hacker who controls the bots may spy, copy and transmit sensitive data, and organize the bots in a swarm attack against targeted computers.” Natasha Solce, supra note 43, at 305.
that exponentially cause websites to crash, or alternatively damage the websites’ host hardware.53

The second kind of cyber attack is the semantic attack.54 Semantic attacks alter the information the computer has access to: a weapon of misinformation.55 “The semantic attack targets the information, substituting inaccurate or misleading information.”56 In particular, the Logic Bomb is one of the most dangerous semantic attacks.57 By implication their composition is that of a bomb: planted in a targeted area and ignited upon desire. Once ignited, Logic Bombs send false data to information systems that can cause them to malfunction.58 The third type of cyber attack is the mixed attack.59 These simply combine syntactic and semantic attacks.60

53 Wolfgang, supra note 50, at 262.
54 Antolin-Jenkins, supra note 34, at 140.
55 See e.g., MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 13 (2009) (“[i]t is possible to attack computers solely at the semantic level by feeding them false information, like lighting a match under a thermostat to chill a room or creating a fake news source.”).
56 Antolin-Jenkins, supra note 34, at 140.
57 See generally, Mark R. Colombell, The Legislative Response to the Evolution of Computer Viruses, 8 RICH. J.L. & TECH. 18 (2002) at http://www.jolt.richmond.edu/v8i3/article18.html (Logic Bombs cause substantial damage before they are ever detected). “Examples include feeding false data to the seismic activity sensing arrays of nuclear plants, causing a shutdown of the plants and a shutoff of significant sources of electrical power, or providing false data to an air traffic control systems, simulating non-existent planes and flight paths, causing confusion and disruption.” Antolin-Jenkins, supra note 34, at 140.
59 Natasha Solce, supra note 43, at 304.
60 Antolin-Jenkins, supra note 34, at 140.
C. THE RISE OF CYBER WARFARE: HACKERS, CYBER CRIMINALS, CYBER TERRORISTS, AND CYBER WARRIORS

Despite the wonders of the Internet, individuals have figured out how to manipulate it.\(^{61}\) Suitably, the actors behind cyber attacks have evolved throughout modern history, starting with hackers, cybercriminals, cyber terrorists, and finally to cyber warriors.\(^{62}\) Hackers\(^{63}\) were the first to learn how to exploit system networks.\(^{64}\) Then, organized crime realized how to monetize the Internet through fraud and personal identity theft.\(^{65}\) Terrorists even used the Internet to further their goals.\(^{66}\) Eventually, militaries around the world imbedded their operations in cyberspace: it became just another domain to conquer.\(^{67}\)

Hackers were the first to venture into the underworld of computer exploitation.\(^{68}\) The definition of a hacker is an individual that uses computers to gain


\(^{62}\) Natasha Solce, *supra* note 43, at 297. “States, criminal organizations, terrorist organizations, and specific individuals are using the developed networks to transverse cyberspace and launch cyber attacks.” Id.

\(^{63}\) See Deirdre Black, *The Computer Hacker- Electronic Vandal or Scout of the Networks?*, 4 J.L. & INF. SCI. 65 (1993) (discussing the characteristics of computer hackers).

\(^{64}\) See Zuley Clark, James Clawson & Maria Cordell, *A Brief History of Hacking* 1—2 (2003) (hacking became a modern trend in the 1980’s with the introduction of the personal computer).

\(^{65}\) Id. at 2.


\(^{67}\) See Aiden Lawes, *Cyber Crime: A 24/7 Global Battle*, ITP REPORT (Nov. 29, 2007) (120 nations have or are developing cyber warfare capabilities).

\(^{68}\) See Cordell, *supra* note 64.
Unauthorized access to data and modify or delete it. Hackers were originally comprised of young adults curious about computer systems. Primarily, hackers infiltrated networks to explore the mechanics of the systems. Subsequently, the trend shifted, as hackers became focused on personal gain, distributing pirated software, computer fraud, and spreading viruses. The case of Kevin Poulsen is illustrative.

In 1994, Poulsen plead guilty to hacking a radio station’s phone system during a radio contest so that it would only let his phone calls through. In short, Poulsen won two Porches, vacations trips, and $20,000 cash. Poulsen was sentenced to fifty-one months in prison for wire and computer fraud, among other

---

71 See Bruce Schneier, supra note 69.
72 See Cordell, supra note 64.
73 See Timeline, supra note 70.
74 Id.
75 Id.
things. The case of Kevin Mitnick is another example. Over a two and half year period, Mitnick allegedly hacked into Motorola, Fujitsu, and Sun Microsystems, stole corporate secrets, broke into the national defense warning system, and stole 20,000 credit card numbers. Mitnick was incarcerated in 1995 on a twenty-five-count indictment, including wire fraud.

Eventually, criminal organizations realized the potential of exploiting the Internet. Cyber crime is generally defined as accessing any computer network with the intent to defraud or to obtain money by means of false representations. The main goal of any cybercriminal is to steal money or acquire information in

76 Id.
78 Id.
79 Id.
80 Debra Wong Yang & Brian M. Hoffstadt, Countering the Cyber-Crime Threat, 43 AM. CRIM. L. REV. 201, 204—05 (2006). “No matter what its core product or service, nearly every business in today’s economy relies upon computers and computer networks to conduct its daily affairs. It is likely that many of a company’s assets—including its trade secrets are archived on these computer systems. If the company’s computer network is accessible to the Internet… those assets are subject to cyber-theft.” Id.
81 See e.g., LA. REV. STAT. ANN. § 14:73.5 (2007).

Computer fraud is the accessing or causing to be accessed of any computer, computer system, computer network, or any part thereof with the intent to: (1) Defraud; or (2) Obtain money, property, or services by means of false or fraudulent conduct, practices, or representations, or through the fraudulent alteration, deletion, or insertion of programs or data.
exchange for money.\footnote{See Natasha Solce, supra note 43, at 301; Wong Yang, supra note 80, at 204. Cyber criminals have also used cyber crime for other than monetary reasons. Press Release, United States Department of Justice, Orange County Man Who Admitted Hacking Into Personal Computers Sentenced to Six Years in Federal Prison for ‘Sextortion’ of Women and Teenage Girls (Sep. 1, 2011) (on file with the Department of Justice) (Luis Mijangos pleaded guilty to computer hacking for using malicious software to hack into teenage girls’ computers, access the victims’ webcams, and take indecent pictures of them. He would subsequently demand sexual favors from the teenage girls in exchange for not releasing the indecent photos. He was sentenced to seventy-two months in federal prison); see also Press Release, United States Department of Justice, Sixteen Individuals Arrested in The United States for Alleged Roles in Cyber Attacks (July. 19, 2011) (In 2010, Wikileaks published large amounts of U.S. State Department cables on its website. In response, PayPal suspended Wikileaks’ account so that it could no longer receive donations. In retribution for PayPal’s termination of Wikileaks’ account, the hacker group Anonymous executed a DDOS attack against PayPal’s computer servers with the intent to damage their network).} In particular, The Russian Business Network (“RBN”) is a cybercrime syndicate that specializes in personal identity theft for resale.\footnote{See Extortion and Denial of Service (DDOS) Attacks, RUSSIAN BUSINESS NETWORK (RBN) BLOG (last visited Oct. 23, 2011), http://rbnexploit.com. Businesses that take an active stance to combat the RBN have been targeted by DDOS attacks. A Walk on the Dark Side: These Badhats May Have Bought Your Bank Account, ECONOMIST, Aug. 30, 2007, available at http://www.economist.com/node/9723768. The RBN generates $150 million in profit per year.} The RBN sells website hosting services to various criminals.\footnote{Brian Krebs, Shadowy Russian Firm Seen as Conduit for Cyber Crime, WASH. POST, Oct. 13, 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html.} They provide exploits to criminal customers, such as fake anti-spyware/anti-malware for the purposes of computer hijacking and identity theft.\footnote{See e.g., David Bizeul, Russian Business Network Study 7 (2007).}
Terrorist organizations have also learned how to exploit the Internet. Cyber terrorism is defined as “the use of computers as weapons, or as targets, by politically motivated international, sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies.” For example, al-Qaeda has been identified as using cyberspace in its jihad against the United States. However, the extent of al-Qaeda’s use of cyberspace has been limited to a supporting role in its operations: using the Internet to communicate, collaborate, recruit, and fundraise for future attacks. Incidentally, Anwar al-Awlaki used Facebook and YouTube to recruit jihadists and to preach for the destruction of the United States.

Terrorist groups have also built online libraries of training materials covering topics including: how sneak through customs, how to make a homemade

---

86 See CARLOS A RODRIGUEZ, CYBERTERRORISM: A RISING THREAT IN THE WESTERN HEMISPHERE 7 (2006). Cyber terrorism is the act of weaponizing computer systems, by politically motivated individuals or groups, to “cause violence and fear in order to influence an audience, or cause a government to change its policies.” Id. The Aum Shinrikyo Cult of Japan stands for the proposition that a terror organization can penetrate the computer networks of a specific target. The Aum Shinriko Cult acquired access to Japanese companies and government agencies by selling them legitimate software “laden with backdoors.” Natasha Solce, supra note 43, at 300. The cult could have entered the companies systems unimpeded and installed computer viruses to launch a cyber attack. See TOM PARKER ET AL., CYBER ADVERSARY CHARACTERIZATION: AUDITING THE HACKER MIND 253 (2004).

87 Natasha Solce, supra note 43, at 301.
88 Id. at 299.
89 Id.
bomb, and how to shoot at a U.S. soldier. 91 Terrorists have also used the Internet to acquire donations to fund their operations. 92 The extremist group Hizb al-Tahrir, for example, used multiple websites throughout Europe and Africa to acquire donations for their jihad. 93

As the actors behind cyber attacks evolved, it was only a matter of time before militaries got involved in cyberspace. 94 First, militaries implemented cyberspace in intelligence gathering. 95 Second, militaries used cyberspace in covert operations, and, eventually, cyber warfare became a modern part of warfare. 96

In its infancy, the Internet was used by militaries for intelligence gathering and espionage. 97 The most

---

93 Id.
94 See e.g., U.S. Cyber Command, UNITED STATES STRATEGIC COMMAND (last visited Nov. 5, 2011) http://www.stratcom.mil/factsheets/cyber_command/ (Established in 2009, Cyber Command “is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks, and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.”).
95 Cf. James Andrew Lewis, The Cyber War Has not Begun, Center For Strategic international Studies 1—3 (2010) (cyberspace is widely used for espionage).
97 See e.g., Nathan Thornburgh, The Invasion of the Chinese Cyberspies, TIME MAGAZINE (2005).
famous example of cyber espionage is allegedly attributable to China against the United States.98 Classified as operation “Titan Rain,” it was a series of ongoing cyber attacks that occurred against United States computer systems beginning in 2003.99 The intrusions allegedly harvested massive amounts of government secrets.100 Equally illustrative is the cyber attack classified as “Moonlight Maze.”101 Russia, through cyber espionage, infiltrated DOD networks for over a year and stole information pertaining to the Department of Energy and NASA.102

Militaries then realized the potential of cyberspace beyond espionage, and they implemented it in covert operations.103 For instance, during the Cold War, CIA agents were able to hack into the industrial control systems of a Soviet gas pipeline.104 The CIA installed a Logic Bomb in the pipeline’s operating system, which caused the software to go haywire.105 The pipeline exploded, causing the biggest non-nuclear explosion in history.106 Recently, Israel hacked into Syria’s air defense systems and disabled them in a covert

98 Id.
99 Shaap, supra note 58, at 141.
101 Shaap, supra note 58, at 141.
102 Id.
103 C.f. John Markoff, A Silent Attack, but Not a Subtle One, N.Y. TIMES, Sep. 26, 2010 (The United States and Israeli Government allegedly used the Stuxnet virus to disrupt the Iranian nuclear program).
104 See generally, Thomas C. Reed, At the Abyss: An Insider’s History of the Cold War (2004).
106 Id.
operation in 2007. 107 Israel then bombed suspected nuclear facilities in Syria.108 The attacks were a complete success because Syria was unaware Israel had attacked.109 The Israeli air force was able to fly over the Syrian airspace with impunity.110

Once governments began using cyber weapons for espionage and covert operations, using cyber weapons in conjunction with actual war naturally followed.111 The 2008 conflict between Russian and Georgia is elucidatory.112 The conflict broke out over South Ossetia, a demilitarized Georgian region on the

109 Id.  
110 Id.  
111 Id.  
112 See Eneken Tikk et al., Cyber Attacks Against Georgia: Legal Lesson Identified 4 (2008); see also Jim Nichol, CSR Report for Congress, Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests 4 (2008) (“In the early 1990s, Georgia and its breakaway South Ossetia region had agreed to a Russian-mediated ceasefire that provided for Russian “peacekeepers” to be stationed in the region. Moscow extended citizenship and passports to most ethnic Ossetians. Simmering long-time tensions erupted on the evening of August 7, 2008, when South Ossetia and Georgia accused each other of launching intense artillery barrages against each other. Georgia claims that South Ossetian forces did not respond to a ceasefire appeal but intensified their shelling, “forcing” Georgia to send in troops. On August 8, Russia launched large-scale air attacks and dispatched troops to South Ossetia that engaged Georgian forces later in the day. By the morning of August 10, Russian troops had occupied the bulk of South Ossetia, reached its border with the rest of Georgia, and were shelling areas across the border. Russian troops occupied several Georgian cities. Russian warships landed troops in Georgia’s breakaway Abkhazia region and took up positions off Georgia’s Black Sea coast.”).
border with Russia. Georgia launched an attack against separatist forces rising up in South Ossetia. Russia responded by sending military forces to protect the Ossetia rebels. Georgia viewed Russia’s military invasion of South Ossetia as a direct act of aggression.

In the weeks leading up to the conflict of South Ossetia, Russia launched a cyber offensive against Georgia. The cyber attacks primarily consisted of propaganda and DDOS attacks. For instance, government websites were defaced and replaced with pictures of Adolph Hitler and Mikheil Saakashvili. Although the propaganda efforts were juvenile, the DDOS attacks had a real effect on the Georgian people. The DDOS attacks crippled government web servers, general e-mail servers, news and media websites, and financial websites. Consequently, the attacks: prevented the Georgians from communicating, causing massive confusion throughout the country; preventing them from acquiring accurate information.

---

113 Tikk, supra note 112, at 4.
114 Nichol, supra note 112, at 4.
115 Id. at 5.
116 Id.
117 Tikk, supra note 112, at 4.
118 Id. at 7.
119 Clarke, supra note 42, at 19.
120 Id. Georgia connects to the Internet primarily through Russia. Id. Because of the DDOS attacks coming into the country, no outbound Internet traffic could get out. Id. Georgians could not connect to outside news sources nor send e-mail out of the country. Id. “Georgia effectively lost control of the nation’s ‘.ge’ domain and was forced to shift many government websites to servers outside the country.” Id.
121 See e.g., John Markoff, Before the Gunfire, Cyberattacks, N.Y. TIMES, Aug. 12, 2008.
about the war escalation; and prevented them from accessing their banking services.

“Whether the world is prepared or not, cyber weapons are becoming a staple of modern war.” This new weapon uses a target nation’s own technology against it to create an asymmetric war. For example, military strategist envision China using cyber attacks against the United States, not in an outright offensive, but to delay the United States long enough for China to seize Taiwan or the disputed islands in the South Sea.

---

123 Tikk, supra note 112, at 8. Georgia’s access to media outlets like CNN and BBC were also blocked. See Clarke, supra note 42, at 18.

124 Tikk, supra note 112, at 8—9. The Georgian banking sector shut down its servers in response to the attacks to prevent from being hacked. Clarke, supra note 42, at 19-20. Russia countered by sending DDOS attacks throughout the international banking community, pretending to be DDOS attacks from Georgia. Id. Foreign banks in response shut down their connection to the Georgian banking sector. Id.

125 Swanson, supra note 122, at 304.

126 Id.; see also QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE: CHINA’S MASTER PLAN TO DESTROY AMERICA 1 (2002) (Asymmetric warfare is a military doctrine in which weaker countries can outmatch traditional military powers by using weapons and tactics that take advantage of weaknesses in superior conventional capabilities).

127 See generally, Jason Fritz, How China Will Use Cyber Warfare to Leapfrog in Military Competiveness, 8 CULTURE MANDALA 28 (2008). “By the end of the 1990s, China’s strategists had converged on the idea that cyber warfare could be used by China to make up for its qualitative military deficiencies when compared to the United States.” Clarke, supra note 42, at 50.

128 See Benjamin Kong, Cyberwar: War in the Fifth Domain, ECONOMIST, July 1, 2010, available at http://www.economist.com/node/16478792/comments. Analyst believe China will find itself with Taiwan in conflict over control of the South Sea. Clarke, supra note 42, at 61. The South Sea is highly sought after because it contains undeveloped oil fields estimated to have more natural gas than Kuwait. Id.
The following hypothetical illustrates how cyber warfare will be used against the United States:

China has aggressively been pressing other Asian countries to cede their rights to the South Sea. The United States learns that China is preparing for an amphibious landing on the disputed islands in the South Sea. In response, the United States dispatches two U.S. battles groups, including twenty ships and over a hundred aircraft, to the region to deter the Chinese. To send a message to the Chinese, the United States hacks the Chinese power grid, causing rolling blackouts throughout the country. In rebuttal, the Chinese: cause black outs throughout Hawaii, California, and Washington; take down the DOD network; and are prepared to launch a broad attack against the United States’ rail network, air traffic control systems, and the financial markets. Realizing the vulnerabilities to the United States, the President is forced to back down and orders the troops to cease offensive action. The Chinese have just used cyber warfare to neutralize the traditional military might of the United States.129

III. DANGERS TO CRITICAL INFRASTRUCTURE

The threat facing the United States is that the United States’ critical infrastructure will be attacked through cyber warfare.130 Critical infrastructure is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any

129 Clarke, supra note 42, at 179—88.
130 Natasha Solce, supra note 43, at 302 (critical infrastructures in the United States are in more danger of attack because they are now connected to the domain of cyberspace).
combination of those matters.” The following sectors have been identified as critical infrastructure: agriculture, food, water, public health, emergency services, defense industrial base, government, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, and postal and shipping.

Cyber attacks pose real dangers to the critical infrastructure of the United States. First, cyber attacks aimed at the energy industry pose significant dangers.

---

131 USA PATRIOT ACT, Pub. L. No. 107—56, 115 Stat. 272 (2001). This paper defines “critical infrastructure” to only encompass the energy, finance, and telecommunications sectors. See e.g., CSIS, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 44 (2008). “These critical cyber sectors are large, interconnected national networks that are the most vulnerable to broad disruption by cyber attack.” Id. at 45. Although water systems, emergency services, transportation networks, and health care services are all vital to the United States, they are decentralized to a local level, and are less likely to be adversely affected from a cyber attack. Id. (“[P]enetrating and disrupting the water supply of one large city, for example, will not disrupt water supplies elsewhere. If these three networks… can continue to operate in the face of attack, the nation can persevere in cyberspace. If they are crippled, online activities will come to an abrupt halt.”). By contrast, damage to energy, finance, or telecommunication sectors would have a debilitating affect on the United States, because they are nationally connected. Id.


133 See e.g., U.S. Gov’t Accountability Office, GAO-11-463T, Cybersecurity: Continued Attention Needed to Protect Our Nation’s Critical Infrastructure and Federal Information Systems 3 (2011). “Federal law enforcement and intelligence agencies have identified multiple sources of threats to our nation’s critical information systems, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors.” Id. “The connectivity between information systems, the Internet, and other infrastructures also creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services.” Id.

134 Id. at 1.
For example, in 2003, the SQL Slammer Worm\textsuperscript{135} was able to infiltrate the network systems in the Ohioan Davis-Besse nuclear power plant.\textsuperscript{136} It was able to corrupt the facilities’ computer control systems for approximately five hours.\textsuperscript{137} Although the breach did not pose any significant safety hazard, the incident illustrates the growing cyber security problem in critical infrastructure.\textsuperscript{138} The Stuxnet virus is also illustrative.\textsuperscript{139}

\textsuperscript{135} \textit{W32.SQLExp.Worm}, SYMANTEC (last visited Nov. 28, 2011), www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99 (The SQL Slammer is a computer worm that indiscriminately spread DDOS attacks across the Internet. The worm was so successful that it dramatically slowed down general Internet traffic).

\textsuperscript{136} Natasha Solce, \textit{supra} note 43, at 302.


\textsuperscript{138} \textit{Id.} (“Experts disagree about the vulnerability of systems that run industrial plants, known as supervisory control and data acquisition (SCADA). But more and more of these are being connected to the internet [sic], raising the risk or remote attack. ‘Smart’ grids,’ which relay information about energy use to utilities, are promoted as ways of reducing energy waste. But they also increase security worries about both crime (e.g., allowing bills to be falsified) and exposing SCADA networks to attack.”). \textit{See} Benjamin Kong, \textit{Cyberwar: War in the Fifth Domain}, ECONOMIST, July 1, 2010, available at http://www.economist.com/node/16478792/comments. Operation Night Dragon is also illustrative of the dangers to critical infrastructure. MCAFEE, \textit{GLOBAL ENERGY CYBER ATTACKS: “NIGHT DRAGON” 3} (2011). Classified as Night Dragon, there have been a series of coordinated cyber attacks that occurred against the oil, energy, and petrochemical sectors since 2009. \textit{Id.} These attacks have utilized vulnerabilities in Microsoft Windows operating systems to harvest sensitive proprietary information. \textit{Id.} The attacks have been attributable to China. \textit{Id.} at 4.

The United States and Israeli government allegedly created Stuxnet to disrupt the Iranian nuclear facility in Natanz.\textsuperscript{140} Stuxnet reportedly infected one fifth of Iran’s nuclear centrifuges causing them to malfunction.\textsuperscript{141} This has reportedly delayed Iran’s ability to create a nuclear bomb.\textsuperscript{142}

\textsuperscript{140} Id. The true identity of the attackers is unknown, yet it is highly suspected that the United States and/or Israel were involved. \textit{Id.} It is suspected that Stuxnet was created by a government entity because the worm was not criminal in design, it was expensive to create, and because the inscription “myrtus” appears in the worm’s code, suggesting Israeli involvement. \textit{Id.} Stuxnet appears to not be criminal designed because the worm does not steal credit card information or herd computers into botnets. \textit{Id.} Because it is estimated that it took eight to ten people six months to create the virus, Stuxnet was most likely financed by a government. \textit{Id.} Further, the word “myrtus” has been linked to Israel because “myrtus” is Hebrew for Hadassah: Queen Esther who saved the Persian Jews from genocide. \textit{Id.}

\textsuperscript{141} Specifically, Stuxnet is an Internet worm that primarily infects computers through USB sticks. Bruce Schneier, \textit{supra} note 139. Once it has gained access to the host computer, it seeks to infiltrate SCADA systems: industrial control systems generally used in critical infrastructure, e.g., the electric power grid, gas pipelines, and nuclear facilities. Pam Benson, \textit{Computer virus Stuxnet a 'game changer,' DHS official tells Senate,} CNN, Nov. 17, 2010, \textit{available at} http://articles.cnn.com/2010-11-17/tech/stuxnet.virus_1_stuxnet-nuclear-power-plants-target?_s=PM:TECH. The worm then manipulates the SCADA systems and sends false instructions to the industrial control systems, causing the systems to malfunction. Bruce Schneier, \textit{supra} note 139.

Second, the financial sectors are also in danger of cyber attacks. In theory, a hostile entity could infiltrate a victim state’s financial sector through a well-crafted cyber attack. Because documentation of wealth and property are generally stored on computer systems, a cyber attack could delete, alter, or crash financial stock markets and paralyze a nation’s economy. However, a cyber attack on the financial industry from a nation-state is unlikely because the “cascade effect of international economic interdependency, deters cyber attacks against...financial programs.” Nonetheless, a cyber attack on the financial industry of any nation is plausible because cyber terrorists are not influenced by economic

143 See U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-03-173, CRITICAL INFRASTRUCTURE PROT.: EFFORTS OF THE FIN. SERV. SECTOR TO ADDRESS CYBER THREATS 22 (2003). Over eighty percent of the financial institutions have had security breaches. Id. Financial losses from stolen proprietary information and fraud are in the hundreds of millions. Id. Specifically, in 1994, a Russian hacker reportedly broke into Citibank’s network and stole $10 million. Id. at 23. Although the hacker was convicted of a felony, Citibank was only able to recover $400,000 of that loss. Id. Additionally, in 2000, two men from Kazakhstan were arrested in London for breaking into Bloomberg L.P.’s computer systems in New York in an attempt to extort $200,000. Id.

144 See e.g., Josh Smith, Financial Industry Especially Vulnerable to Cyberattacks, Analysts Say, NATIONAL JOURNAL, Sep. 14, 2011, http://www.nationaljournal.com/tech/financial-industry-especially-vulnerable-to-cyberattacks-analysts-say-20110914 (“Because financial institutions are critical to the nation’s economic security and handle large sums of money, malicious actors find them to be especially attractive targets.”).

145 CRS REPORT FOR CONGRESS, COMPUTER ATTACK AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 9—11 (2003). “For example, cyber attacks that secretly corrupt secure credit card transaction data at retail Internet sites, could possibly cause that corrupted data to spread into banking systems and could erode public confidence in the financial sector, or in other computer systems used for global commerce.” Id.

146 Natasha Solce, supra note 43, at 310.
deterrence.\textsuperscript{147} Thus, the financial sector could be a possible target.\textsuperscript{148}

Third, the dangers posed to civilian government infrastructure are apparent.\textsuperscript{149} As governments become more connected, they will be more vulnerable to cyber attacks.\textsuperscript{150} The case of Estonia, “e-Stonia,”\textsuperscript{151} is especially elucidatory.\textsuperscript{152} By 2007, Estonia had implemented an online government where ninety percent of governmental services were conducted online.\textsuperscript{153} Estonians conducted most banking through online services, voted for parliamentary elections online, and mostly communicated through Skype, an Internet phone system.\textsuperscript{154} Estonia’s dependence on the Internet made cyber attacks against it extremely effective.\textsuperscript{155} The cyber attacks occurred because Estonia decided to relocate the Bronze Soldier Tallinn, a soviet-era grave marker honoring fallen soviet soldiers during World War II.\textsuperscript{156} In protest, thousands of DDOS attacks from Russia flooded Estonia.\textsuperscript{157} The attacks brought down critical

\begin{footnotesize}
\begin{enumerate}
\item[147] Id.
\item[148] C.f. Smith, supra note 144.
\item[149] See Joshua Davis, Hackers Take Down the Most Wired Country in Europe, WIRED MAGAZINE, Aug. 21, 2007.
\item[150] See e.g., Myriam Dunn Cavelty, Critical information infrastructure: vulnerabilities, threats and responses 17 (2007).
\item[153] Id.
\item[154] Id.
\item[155] Id.
\item[156] Davis, supra note 149.
\item[157] Shackelford, supra note 152, at 193.
\end{enumerate}
\end{footnotesize}
In review, critical infrastructures are defined as those infrastructures so vital to the United States that their destruction would debilitate the country. Cyber attacks have been able to infiltrate nuclear power plants and pose security threats to the electric grid. The financial sector could be decimated by an orchestrated cyber attack. Additionally, disruptions to government infrastructure can lead to mass confusion and social unrest. The foregoing evidences the dangers cyber attacks pose to critical infrastructure.

IV. THE LAWLESSNESS OF CYBER WARFARE AND WHY CYBER WARFARE WILL NOT BE STOPPED

No international treaty governs cyber warfare. Consequently, nations must practice law by analogy, applying various legal theories to cyber attacks. However, applying other theories to cyber warfare by analogy does not provide a workable model to govern governmental websites and caused social unrest and rioting.  

158 Id. at 194.
160 See e.g., Schneier, supra note 139.
161 See Smith, supra note 144.
162 Shackelford, supra note 152, at 193.
163 See e.g., George Kurtz, Critical Infrastructure Not Ready For Cyberattacks, MCAFEE BLOG CENTRAL (April 20, 2011, 12:38 PM), http://blogs.mcafee.com/corporate/cto/critical-infrastructure-not-ready-for-cyberattacks (there is an increased danger to the oil, gas, power, and water industries).
165 Carr, supra note 44, at 47.
cyber warfare.\textsuperscript{166} Alternatively, if actual international legislation is agreed upon to govern cyber warfare, cyber warfare will continue because the responsibility for cyber attacks cannot be attributable to a nation-state, regulating cyber warfare would be impractical, and because weaker military nations will use cyber warfare to combat larger military forces.\textsuperscript{167}

A. THE FIRST RULE OF CYBER WARFARE, THERE ARE NO RULES OF CYBER WARFARE

The law of cyber warfare is in unclear.\textsuperscript{168} “Right now, no comprehensive international treaty exists to regulate cyber attacks. Consequently, states must practice law by analogy either equating cyber attacks to traditional armed attacks and responding to them under the law of war or equating them to criminal activity and dealing with them under domestic criminal laws.”\textsuperscript{169} Currently, academics have theorized that cyber warfare could be internationally governed by analogizing it to: (1) the Nuclear Non-Proliferation Treaty, (2) the United Nations Charter, or (3) the Outer Space Treaty or the


\textsuperscript{167} See infra Part III-B.

\textsuperscript{168} Carr, \textit{supra} note 44, at 47.

\textsuperscript{169} \textit{Id.}
Antarctic Treaty System.\textsuperscript{170} This article argues that none of these analogies provides a workable model to govern cyber warfare.\textsuperscript{171}

\textsuperscript{170} See e.g., Shackelford, \textit{supra} note 152, at 150. Some theorists have explained that Mutual Legal Assistance Treaties (“MLATs”) could govern cyber warfare. See generally, Carr, \textit{supra} note 44. MLATs encompass everything from diplomatic relations, extradition, or legal assistance. Shackelford, \textit{supra} note 152, at 228. Specifically, they can be applied to seek criminal prosecution of individuals responsible for cyber attacks, and their extradition to a requesting nation. Shackelford, \textit{supra} note 152, at 228. For example, the Convention on Cybercrime is the first international treaty to address cybercrime by standardizing national laws. See e.g., Amile M. Weber, \textit{The Council of Europe’s Convention on Cybercrime}, 18 BERKELEY TECH. L.J. 425 (2003). The convention mandates a list of crimes that each signatory must create into their own law: criminalization of hacking, Internet child pornography, and the increase of liability for intellectual property violations. Budapest, 23.XI.2001. The convention also requires signatory nations to provide international cooperation for international cyber crimes, including the collection of evidence, and the police assistance from participating nations. \textit{Id.} This paper does not address MLATs because they pertain to criminal matters. Accordingly, they have no weight in addressing international warfare.

Theorists have also analogized the law of the sea to cyberspace. See Shackelford, \textit{supra} note 152, at 227. According to UNCLOS Article 19, nations have an obligation to not engage in activities “prejudicial to the peace, good order, or security of the coastal [s]tate.” See United Nations Convention on the Law of the Sea art. 19, Dec. 10, 1982, 1833 U.N.T.S. 243; see also Shackelford, \textit{supra} note 152 at 227 (Nations also have an obligation not to engage in activities such as the collection of information, propaganda, or interfering with telecommunications systems). Additionally, UNCLOS Article 113 requires domestic criminal legislation to penalize intentional damage to submarine cables. United Nations Convention on the Law of the Sea art. 13, Dec. 10, 1982, 1833 U.N.T.S. 243. Applied to cyberspace, “this means that cyber attackers who send code through submarine cables to a coastal state would be in breach of international law obligations.” Shackelford, \textit{supra} note 152, at 227. Similar to MLAT, UNCLOS enforcement mechanism is based on criminal law enforcement and is not addressed in this article.
1. THE NUCLEAR NON-PROLIFERATION TREATY

Some academics have compared nuclear weapons to that of an escalated cyber attack. Accordingly, theorists have suggested that it would be appropriate for a nonproliferation treaty to regulate cyber warfare. For example, the Nuclear Non-Proliferation Treaty (“NPT”) is an international agreement to limit the spread of nuclear weapons. Each member of the treaty agrees to not transfer nuclear weapons, nor induce any non-nuclear weapon state from developing nuclear weapons. The members also agree to be regulated by the International Atomic Energy Agency (“IAEA”) to

---

171 See Charles J. Dunlap, Towards A Cyberspace Legal Regime in the Twenty-First Century: Consideration for American Cyber Warriors, 87 NEB. L. REV. 712, 714 (discussing the complexities in applying existing law to cyber war issues).

172 Cyber attacks have been compared to weapons of mass destruction. See e.g., Shackelford, supra note 152, at 150, 216 (the Russians have also stated that an attack against the United States’ telecommunications and electric grid would necessarily overlap with the use of weapons of mass destruction); see also Paul Mann, Cyber-threat Expands with Unchecked Speed, 145 AVIATION WEEK & SPACE TECH. 63, 64 (1996) (According to former CIA Director John Deutch, cyber warfare is categorized slightly under nuclear, biological, or chemical weapons). Both types of attacks would be unable to distinguish between the civilian and military populations. Shackelford, supra note 152, at 218. Further, both types of attacks would “destroy all critical infrastructures, leave the victim nation completely helpless and terrorize its population.” Id. “Some of the effects of nuclear weapons can be similar to a worst-case cyber attack on a state. An all-out attack could disable or destroy all critical infrastructures, leave the victim nation completely helpless and terrorize its population.” Id. Cyber attacks may be even more harmful to the civilian population because of the anticipated focus on critical infrastructure. Shackelford, supra note 152, at 219.

173 Shackelford, supra note 152, at 219.


175 Id.
verify that they are not diverting nuclear energy from peaceful use to explosive devices. A cyber warfare nonproliferation treaty could stop the escalation of cyber warfare, ban the creation of cyber weapons, and protect the international community by regulated safeguards.

Although a nonproliferation treaty could be applied to cyber warfare in theory, the implementation of the treaty would be unworkable because: (a) there is no international oversight agency that could regulate cyber warfare, and (b) cyber weapons cannot be verified by independent government reconnaissance. First, the NPT is enforceable because the materials required to create a nuclear device are rare. Because nuclear materials are rare, the IAEA is able to monitor and trace them. Conversely, the creation of cyber weapons is vast because it only requires programmers and computer hardware. The abundance of cyber weapons makes it impractical to trace them. Further, regulators would need access to all computer databases within a nation, and have the resources to search through billions of lines of code. This is impractical because malicious code

---

178 Carr, supra note 44, at 32.
179 Id.
181 Shackelford, supra note 152, at 217. “This difficulty stems from the fact that the computer code that compromise IW are often indistinguishable from innocent information requests.” Id.
created for cyber warfare is often indistinguishable from other innocent data.  

Second, nation-states would not be able to verify the existence of cyber weapons through traditional intelligence gathering. The NPT is also enforcable because nations can independently determine nuclear activity in other countries, e.g., spy satellites can verify the creation of nuclear weapons programs. Conversely, cyber weapons can be made anywhere there is an Internet connection. Cyber warriors operate completely invisible from the international community.

2. THE UNITED NATIONS CHARTER

Other academics have proposed that the United Nations Charter ("U.N. Charter") could govern cyber warfare. The U.N. Charter and customary international law governs the use of force by states. It provides the legal framework to understand the availability and limitations on the use of force. Accordingly, theorists

---

183 Shackelford, supra note 152, at 217.
184 See infra Part III-B.
185 See e.g., David E. Sanger & William J. Broad, Watchdog Finds Evidence That Iran Worked on Nuclear Triggers, N.Y. TIMES, May 24, 2011.
187 Id.
188 See e.g., Shaap, supra note 58, at 142.
190 McGavran, supra note 50, at 269.
suggested that it is appropriate to apply the U.N. Charter to cyber warfare.\footnote{Id.}

The U.N. Charter prohibits the use of force unless two exceptions apply.\footnote{Id.} According to Article 2(4) of the U.N. Charter: “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.” (emphasis added).\footnote{U.N. Charter art. 2(4).}

The two exceptions to the prohibition on the use of force are as follows.\footnote{See Herbert S. Lin, Offensive Cyber Operations and the Use of Force, 4 J. Nat’l Sec. L. & Pol’y 63, 71 (2010).} First, Article 42 permits the Security Council to authorize the use of force to combat any threat to the peace or an act of aggression in order to bring international stability.\footnote{U.N. Charter art. 42.} Second, Article 51 provides: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.” (emphasis added).\footnote{U.N. Charter art. 51.}

Unfortunately, the U.N. Charter does not define “use of force” or “armed attack.”\footnote{Lin, supra note 194, at 71.} Nonetheless, there is an international consensus that “use of force” or “armed

\footnote{Id. The Law of Armed Conflict (“LOAC”) provides the legal framework for modern warfare. Lin, infra note 194, at 71. The LOAC is divided into two separate bodies of law: jus ad bellum—when it is legal for one nation to use force against another—and jus in bello—the rules that govern nations once they are engaged in war. Id. The U.N. Charter and customary international law govern jus ad bellum. Id. .}

\footnote{Id.}

\footnote{U.N. Charter art. 2(4).}

\footnote{See Herbert S. Lin, Offensive Cyber Operations and the Use of Force, 4 J. Nat’l Sec. L. & Pol’y 63, 71 (2010).}

\footnote{U.N. Charter art. 42.}

\footnote{U.N. Charter art. 51.}

\footnote{Lin, supra note 194, at 71.}
attack” means “military force.” For example, declaring war, the occupation of territory, or naval blockades would constitute an armed attack. However, economic coercion would not constitute a use of force. For instance, economic sanctions, space-based surveillance, espionage, or political coercion do not amount to a “use of force.”

Regrettably, there is no consensus for how cyber attacks should be regarded under the U.N. Charter. The first issue is whether a cyber attack can amount to a “use of force” under Article 2(4), or an “armed attack” under Article 51 giving rise to a right of self-defense. Most academics generally believe that a cyber attack could amount to a use of force or an armed attack if it is severe enough. Accordingly, the next problem is

198 Id. It is assumed that unfriendly actions such as “unfavorable trade decisions, space-based surveillance, boycotts, severances of diplomatic relations, denial of communications, espionage, economic competition or sanctions, and economic and political coercion do not rise to the threshold of a use of force, regardless of the scale of their effects.” Id. at 71—72. See also Nicaragua v. United States, 1986 I.C.J. 14, 106 (June 27) (“every sovereign [s]tate [has a right] to conduct its affairs without outside interference… [this] is part and parcel of customary international law.”).
199 Lin, supra note 194, at 71.
200 Id.
201 Id.
203 Id.; McGavran, supra note 50, at 269—70. There are three approaches in analyzing cyber attacks under the U.N. Charter. Id. The “Instrumentality approach” would define cyber attacks as being outside the definition of “force” because they are inherently different from kinetic attacks. Id. Under the “Target approach,” cyber attacks would constitute “force” if they were able to penetrate critical infrastructures within a nation. Id. Under the “Consequentiality approach,” a cyber attack would constitute “force” if it were able to replicate the same damage a traditional kinetic attack could. Id.
204 Michael N. Schmitt, Computer network attack and the use of force in international law: thoughts on a normative framework.
determining between cyber attacks that are military force or economic coercion.\textsuperscript{205}

The application of the U.N. Charter to cyber warfare is problematic because cyber warfare can be defined as both military force and economic force.\textsuperscript{206} The majority view among international scholars is that “use of force” only encompasses the use of military force, \textit{i.e.}, kinetic attacks.\textsuperscript{207} Economic coercion, such as sanctions, is excluded from the definition.\textsuperscript{208} A cyber attack can be classified as military force because it could physically, through virtual cyber attacks, destroy operating systems, destroy economic infrastructure, and paralyze a nation’s wealth.\textsuperscript{209} Alternatively, a cyber attack can also be classified as economic coercion because it could affect the economic infrastructure of a nation by attacking financial markets or otherwise disrupting an economy.\textsuperscript{210}

The following is an example that illustrates the problem in determining whether a cyber attack is military force or economic coercion:

Bombps dropped on [the United States’] stock exchange at night, so that casualties were minimized, would be regarded as a use of force or armed attack by most observers, even if physical backup facilities were promptly available so that actual trading was disrupted for only a few hours. The

\textsuperscript{206} Id. at 422.
\textsuperscript{207} See LIEUTENANT COLONEL SCOTT W. BEIDLEMAN, DEFINING AND DETERRING CYBER WAR 15 (2009); see also Antolin-Jenkins, supra note 34, at 152—53.
\textsuperscript{208} Id.
\textsuperscript{209} Id.
\textsuperscript{210} C.f. Antolin-Jenkins, supra note 34, at 155.
posed cyber attack could have the same economic effects, except that the buildings themselves would not be destroyed. In this case, the cyber attack may be less likely to be regarded as a use of force than a kinetic attack with the same (temporary) economic effect, simply because the lack of physical destruction would reduce the scale of the damage caused. However, a cyber attack against the stock exchanges that occurs repeatedly and continually, so that trading is disrupted for an extended period of time, for days or weeks, would surely constitute a use of force or even an armed attack, even if no buildings were destroyed.211

Because of the difficulty in determining whether a cyber attack is a military force or an economic force, resolving whether a cyber attack is a use of force or armed attack must be determined on a case-by-case basis.212 “Some commentators have charted a spectrum of action, where a minor incursion into the sovereign territory of a state with a minimum use of force does not give rise to right to act in self-defense, whereas a more robust action, either causing significant destruction or targeting, does.”213 For example, electronic espionage and the interruption of telecommunications systems may not amount to an armed attack, where a DDOS attack

211 Lin, supra note 194, at 74.
212 WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 135—42 (1999). “The terms ‘use of force,’ ‘armed attack,’ and ‘self-defense’ will never be clearly defined by objective rules of law. The international community has struggled for decades to define these terms, but there are simply too many factual variables involved to capture them in a few simple rules.” Id. at 138.
213 Antolin-Jenkins, supra note 34, at 162.
could. However, the determination of what constitutes military force or economic coercion would still be arbitrary.

Further, enforcing cyber warfare under the U.N. Charter would be challenging because it is difficult to attribute responsibility for cyber attacks. The problem with cyber warfare is that it is extremely difficult to attribute an attack to a specific actor or to determine the intent behind the attack. The U.N. Charter would only deter cyber warfare if states could retaliate when they have been the victims of a cyber attack. Because states cannot attribute responsibility for an attack against them, they will be unable to respond with military action. The lack of attribution in a cyber attack renders the U.N. Charter of limited use.

Retaliation also requires attribution because it ensures that the retaliating state will not target innocent

---

214 Joshua E. Kastenberg, Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law, 64 A.F. L. REV. 43, 55 (2009) (the majority of the international community agrees that cyber attacks, such as DDOS attacks, violate the international principle of neutrality).


217 Todd C. Huntley, Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare, 60 NAVAL L. REV. 1, 13 (2010) (“Lacking the capability to determine the intent of the perpetrator makes it almost impossible to structure an appropriate, lawful response, and is likely to leaving a state guessing as to whether it was facing an imminent cyber attack or merely a teen-ager taking the family computer for a spin.”).

218 C.f. Shackelford, supra note 152, at 200.

219 Id.

entities. A nation quick to react to an attack might wage war with another nation who they suspect is responsible, where in reality the attack came from somewhere else. Further, retaliation requires attribution, because the laws governing self-defense depend on whether the attacker is a state actor or non-state actor. Retaliation in self-defense must comply with the U.N. Charter if the attacker is a state actor. However, if the attacker is a non-state entity then criminal law will govern the response measures. The victim state needs to be able to immediately attribute responsibility for the attack in order to comply with the legality of self-defense. Therefore, nation-states need to be able to attribute responsibility for cyber attacks for the U.N. Charter to be enforceable.

222 Id.
223 Id.
224 Id.
225 Id. at 415; see also Daniel M. Creekman, Note, A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks From China, 17 AM. U. INT’L L. REV. 641, 661 (2002).
226 Condron, supra note 221, at 415.
227 Id.
3. THE OUTER SPACE TREATY AND THE ANTARCTIC TREATY SYSTEM

Cyberspace is sometimes referred to as an international “commons,” comparable to outer space or Antarctica. Accordingly, some theorists have explained that cyber warfare could be governed by analogy to the Outer Space Treaty (“OST”), or the Antarctic Treaty System (“ATS”).

i. **The Outer Space Treaty**

Theorists have explained space law could govern cyber warfare. The OST states that “outer space, including the Moon and other celestial bodies” are not subject to a “claim of sovereignty, by means of use or occupation, or by any other means.” The OST does

---

228 See Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 A.F. L. REV. 1, 14—18 (2009) (discussing cyberspace under a global commons theory); Shackelford, *supra* note 152, at 213 (“As applied to cyberspace, this means that although computer networks owned by the private and public sectors provide the infrastructure for the information superhighway, they cannot actually own the data packets (the cars) on the Internet. Thus, the various government institutions and telecommunications firms that issue Internet protocol (IP) addresses within their countries do in a sense own Internet Access, but not the Internet itself.”); but see James A. Lewis, *Sovereignty and the Role of Government in Cyberspace*, 16 BROWN J. WORLD AFF. 55, 62 (2009) (although ownership of Internet networks are fragmented, ownership and sovereignty still exists, even if it is not usually enforced).

229 See Carr, *supra* note 44, at 33 (the comparisons to outer space are evident; both boundless and unregulated).


231 *Id.*

not prohibit the militarization of space.\textsuperscript{233} It only prohibits placing nuclear weapons, or weapons of mass destruction, in orbit, or placing them on celestial bodies.\textsuperscript{234} Application of the OST to cyber warfare would prevent the Internet from becoming nationalized and prohibit cyber weapons of mass destruction in cyberspace.\textsuperscript{235}

Unfortunately, analogizing the OST to cyber warfare provides an inadequate model to govern cyber warfare.\textsuperscript{236} First, the analogy of cyberspace to outer space is tenuous: cyberspace is not a “commons,” but it is network of privatized networks.\textsuperscript{237} More importantly, it is unclear how the OST would be applied:\textsuperscript{238} Can nations militarize cyberspace, so long as their cyber weapons do not rise to the level of nuclear weapons? Assuming the affirmative, what kind of cyber attack would rise to the level of a nuclear weapon? Because it is unlikely that a cyber attack could equate to a nuclear weapon, applying the OST to cyber warfare would actually permit the militarization of cyberspace.\textsuperscript{239}

Further, enforcing an outer space-type treaty would be difficult because cyber weapons are hard to

\begin{itemize}
\item \textsuperscript{233} Shackelford, \textit{supra} note 152, at 220 (“The military use of space was not completely forbidden by the 1967 U.N. Outer Space Treaty, as evidenced by the existence of earth-orbit military reconnaissance satellites, remote-sensing satellites, military global-positioning systems, and space-based aspects of an antiballistic missile system.”).
\item \textsuperscript{234} The Outer Space Treaty art. 5, Jan. 1, 1967, 610 U.N.T.S. 205.
\item \textsuperscript{235} \textit{C.f. Id.}
\item \textsuperscript{237} \textit{Reno,} 929 F. Supp. at 830.
\item \textsuperscript{238} Carr, \textit{supra} note 44, at 33.
\item \textsuperscript{239} Shackelford, \textit{supra} note 152, at 222.
\end{itemize}
trace. The OST is enforceable because it is easy to attribute responsibility for weapons in space. In contrast, locating cyber weapons in cyberspace would require finding a single strand of malicious code in billions of lines of code and then determining who created the code. Attributing responsibility for space weapons is also practical because only a few nations have space capabilities. Conversely, one hundred and twenty nations have the capability to engage in cyber warfare. Therefore, the OST model, as applied to cyber warfare, would be difficult to enforce.

**ii. The Antarctic Treaty System**

Theorists have also explained that the ATS could be applied to cyber warfare. The ATS establishes Antarctica as a scientific preserve and bans

---

240 Carr, *supra* note 44, at 33.
241 *Id.*
242 *Id.*
243 *Id.*
244 *Id.*
245 *Id.*
246 *Id.; see also* Menthe, *supra* note 230, at 88 (analogizing the law of Antarctica to cyberspace). “The Antarctic Treaty, the earliest of the post-World War II arms limitation agreements, has significance both in itself and as a precedent. It demilitarized the Antarctic Continent and provided for its cooperative exploration and future use. It has been cited as an example of nations exercising foresight and working in concert to prevent conflict before it develops. Based on the premise that to exclude armaments is easier than to eliminate or control them once they have been introduced, the treaty served as a model, in its approach and even in its specific provisions, for later ‘non-armament’ treaties -- the treaties that excluded nuclear weapons from outer space, from Latin America, and from the seabed.” U.S. DEP’T OF STATE, http://www.state.gov/t/isn/4700.htm (last visited Nov. 24, 2011).
all military activity on the continent.\textsuperscript{247} The purpose of the treaty is assurance “that Antarctica shall continue forever to be used exclusively for peaceful purposes and shall not become the scene or object of international discord.”\textsuperscript{248} Applying the ATS to cyber warfare would mean preserving cyberspace by banning all cyber weapons in cyberspace.\textsuperscript{249}

Lamentably, applying the ATS to cyber warfare is problematic and unworkable.\textsuperscript{250} The application of the ATS to cyber warfare would hinder Internet innovation.\textsuperscript{251} The ban on cyber weapons would be a detriment to the Internet because “imposing such a freeze on developing new software capable of malicious attacks…stifles innovation.”\textsuperscript{252} The enforcement of the ATS-model would also be questionable because it is impractical to identify malicious code in cyberspace;\textsuperscript{253} Antarctica has definite borders whereas cyberspace is limitless.\textsuperscript{254} Consequently, the application of the ATS to cyber warfare provides a difficult model to implement.\textsuperscript{255}

\textit{iii. Space Law and Antarctic Treaty in Review}

To conclude, applying the OST or the ATS to cyber warfare would not provide a workable structure to govern cyber warfare.\textsuperscript{256} First, it is uncertain how the

\begin{itemize}
\item \textsuperscript{247} The Antarctic Treaty art. 1, Dec. 1, 1959, 402 U.N.T.S. 73. “Rather than banning only the most egregious cyber use, it may be more thorough to regulate all hacking that could become a cyber attack.” Shackelford, \textit{supra} note 152, at 221.
\item \textsuperscript{248} The Antarctic Treaty, Dec. 1, 1959, 402 U.N.T.S. 73.
\item \textsuperscript{249} Carr, \textit{supra} note 44, at 33.
\item \textsuperscript{250} \textit{Id}.
\item \textsuperscript{251} Shackelford, \textit{supra} note 152, at 222.
\item \textsuperscript{252} \textit{Id}.
\item \textsuperscript{253} Carr, \textit{supra} note 44, at 33.
\item \textsuperscript{254} \textit{Id}.
\item \textsuperscript{255} \textit{Id}.
\item \textsuperscript{256} \textit{See supra} Part III-A-3.
\end{itemize}
applications will functionally work. Second, it is difficult to enforce the applications because it is hard to police cyber weapons and attribute responsibility for them. Third, the applications could stifle Internet innovation. For the foregoing reasons, the OST or the ATS do not provide adequate legal analogies to regulate cyber warfare.

B. CYBER WARFARE IS HERE TO STAY

Assuming a comprehensive international treaty is agreed upon to specifically govern cyber warfare, nations will continue to use cyber warfare regardless of the treaty. Nations will reserve cyber warfare as part of their military operations because: (1) attributing responsibility for cyber attacks is problematic; (2) cyber warfare regulations cannot be enforced; (3) the decentralized nature of the Internet fosters cyber exploitation; (4) most cyber attacks go unreported; (5) the entry costs of cyber warfare is minimal; (6) cyber warfare can be used to coerce superior military forces into asymmetric warfare; and (7) attacking a nation’s critical infrastructure destroys the victim state’s internal operational viability.

Nations will use cyber warfare to conduct military operations because attributing responsibility for cyber attacks is problematic. First, determining the

257 Id.
258 Id.
259 Id.
260 Id.
261 See Swaine, supra note 96.
262 See infra Part III-B.
263 Attribution in Cyber Attacks is Difficult, But Not Impossible, SECURE NATION (Feb. 4, 2010), http://securenation.wordpress.com/2010/02/27/attribution-in-cyber-attacks-is-difficult-but-not-impossible/ (Although there is no technology that can automatically determine an attack origin, it is possible to identify the attackers through traditional detective work).
location where the cyber attack originated is challenging.\textsuperscript{264} Cyber attackers deliberately disguise the origin of their attacks by rerouting them through various Internet servers.\textsuperscript{265} Generally, cyberwarriors route their attacks through innocent servers—“stepping stones”—located throughout the world.\textsuperscript{266} For example, an attack traced to Russian servers is not determinative that the attack originated from Russia.\textsuperscript{267} The attack might actually be from Estonia, New Zealand, or the United States, using Russia as a stepping-stone to conceal the originating nation’s true identity.\textsuperscript{268} Therefore, attribution cannot be conclusively determined through evidence of attack origin.\textsuperscript{269}

Second, determining the identity of the attacker is full of twists and turns.\textsuperscript{270} Although cyber attacks may be traced to a particular nation, the government, terrorists, or criminals may be responsible for the attacks.\textsuperscript{271} Conclusively ascertaining the identity of the attacker requires an intensive investigation with the assistance of the forum state.\textsuperscript{272} However, it is unlikely the forum state will give assistance, because it is common for states to incite cybercriminals within their territory to commit cyber attacks against other nation-

\begin{footnotes}
\item[264] Shackelford, \textit{supra} note 152, at 203—09 (“There are no flags or tanks in a cyber attack and the identity of the perpetrators is likely concealed.”).
\item[265] Id.
\item[267] Id.
\item[268] Id.
\item[269] Id.
\item[270] Shackelford, \textit{supra} note 152, at 200—01.
\item[271] Id.
\item[272] \textit{See} Carr, \textit{supra} note 44, at 47 (Russia and China harbor cyber attackers).
\end{footnotes}
states.\textsuperscript{273} These harbor states then hide behind their cyber minions in a “veil of plausible deniability and thus escape accountability.”\textsuperscript{274}

Nations will conduct cyber warfare, because cyber warfare regulations are realistically unenforceable.\textsuperscript{275} Until a cyber attack is launched, regulators would not be able to police cyber warfare, rendering them completely useless in peacetime.\textsuperscript{276} Regulators would need access to all computer databases within the forum state because attacks could originate from any server within the forum state.\textsuperscript{277} If that were possible, regulators would then need to be able to identify malicious code through billions of lines of computer data.\textsuperscript{278} “To spot a cyber attacker from all the normal cross-border data flows would be like picking out a single person with more luggage than usual from the thousands of passengers that pass through JFK Airport daily.”\textsuperscript{279}

\textsuperscript{273} McAfee, Virtual Criminology Report: Cybercrime Versus Cyberlaw 15 (2008).
\textsuperscript{274} See Shackelford, supra note 152, at 233. In return for their services, the cyber attackers, assuming they can be identified, are likely to receive asylum within the forum state. McAfee, supra note 273, at 15. Russia and China provide a safe haven to individuals suspected of committing cyber attacks within their territories. Id. The implication is that Russia and China’s intelligence agencies are protecting the country’s cybercriminals. Id.
\textsuperscript{275} See generally, McGavran, supra note 50, at 268.
\textsuperscript{276} See supra Part III-A. Regulators may conduct a cyber forensic investigation once cyber attacks occur. Until then, however, regulators would have to sit on their hands, figuratively speaking.
\textsuperscript{278} Shackelford, supra note 152, at 200.
\textsuperscript{279} Id.
Nations will continue to use cyber warfare because of the loose nature of the Internet.\textsuperscript{280} The Internet fosters an environment of porous security, resulting in network vulnerabilities.\textsuperscript{281} This is mainly because the Internet was designed to be a decentralized collaborative communications system.\textsuperscript{282} Security and identity management were not structural priorities.\textsuperscript{283} As a result, cybersecurity will always be one step behind cyber attackers.\textsuperscript{284} Cyber attackers will eventually find vulnerabilities and defeat security measures put in place to prevent cyber attacks.\textsuperscript{285}

Nations will implement cyber warfare because most cyber intrusions go unreported and many more are not even detected, which allows the attackers to escape accountability.\textsuperscript{286} Currently, approximately ninety percent of cyber attacks go unreported.\textsuperscript{287} Apparently, corporations would rather absorb the costs of cyber

\begin{footnotesize}
\begin{enumerate}
\item See Natasha Solce, supra note 43, at 307 (discussing a non-exhaustive list of why cyber attacks will occur).
\item Id.
\item See William F. Lynn III, Defending a New Domain: The Pentagon's Cyberstrategy, 89 FOREIGN AFF. 97, 99 (2010).
\item Id.
\item Id.
\item Id.
\item Id.
\item Id.
\item See Kevin Voigt, Analysis: The Hidden Cost of Cybercrime, CNN (June 7, 2011), http://edition.cnn.com/2011/BUSINESS/06/06/cybercrime.cost/index.html (organizations are cautious to publicize breaches to their corporate security). Recently, there have been many high profile cyber attacks against large organizations. Id. For example, Sony’s PlayStation Network was compromised in May 2011, resulting in $171 million in damage. Id. Lockheed Martin and Google’s computer networks were also recently breached. Id.
\item Natasha Solce, supra note 43, at 307 (at least eighty percent of security intrusions go unreported); Marc Goodman & Susan W. Brenner, Emerging Consensus on Criminal Conduct in Cyberspace, 10 Int’l J.L. & Info. Tech. 139, 157 (2002) (only ten percent of cyber attacks are reported to any kind of authority).
\end{enumerate}
\end{footnotesize}
attacks than face the negative publicity that their systems have been compromised. Further, cyber attacks are covert and do not leave easily identifiable evidence of their assault. As a result, most organizations are unaware their networks have even been infiltrated. This allows hackers to commit attacks with practical impunity.

Additionally, cyber attacks will become increasingly used in modern warfare because of its low costs. Cyber warfare is inexpensive relative to the costs of developing and maintaining twenty-first century kinetic weapons. Because the battlefield of cyber warfare occurs over publically accessible networks, the only expenses incurred to conduct cyber war pertain to training cyber warriors and acquiring the computer hardware needed to launch cyber attacks. “The low entry cost of cyberspace appeals to nations, criminals, and terrorist organizations that cannot outmatch or inflict

288 Goodman, supra note 287, at 157.
289 Id; see also David Goldman, Massive hack hit 760 companies, CNN MONEY, Oct. 28, 2011, http://money.cnn.com/2011/10/27/technology/rsa_hack_widespread/index.htm (multiple fortune 500 companies were victims of cyber attacks recently, and most of these companies were probably unaware of the attacks).
290 Martin Sutherland, Know your enemy, know your risk, NEW EUROPE, June 12—18, 2011, at 10.
293 See, e.g., MARTIN C. LIBICKI, RAND CORPORATION, Cyb erdeterrence and Cyberwar xvi, 177 (2009). “Because a devastating cyber attack may facilitate or amplify physical operations and because an operational cyber war capability is relatively inexpensive (especially if the Air Force can leverage investments in CNE), an offensive cyber-war capability is worth developing.” Id.
294 See Brenner, supra note 292, at 250.
harm upon the United States in an alternative manner.”

Furthermore, nations will use cyber warfare because it can force a stronger military power into asymmetric warfare. Opponents will not challenge the United States’ traditional military superiority. The United States allocates more to defense spending than the next seventeen largest nations combined. Because of this, militaries will instead resort to asymmetric tactics and exploit the United States’ vulnerabilities in cyberspace.

Cyber warfare is now the “great equalizer,” because weaker military nations can now defend

---

298 Daily Chart Blog, supra note 297.
themselves through cyberspace. \(^{301}\) Nations no longer need to acquire expensive stockpiles of weapons, such as stealth fighters, to counteract the United States’ military capabilities. \(^{302}\) “A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States’ global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target.” \(^{303}\)

Lastly, nations will resort to cyber warfare because attacking a nation’s critical infrastructure destroys the victim state’s internal operational viability. \(^{304}\) Attacking critical infrastructure, such as power, emergency response systems, or banking, would

\(^{301}\) See Kamal, supra note 6, at 78. “Current military theory suggests therefore that attacking a nation’s center of gravity, in addition to its armed forces, is the most effective way to destroy the state. In today’s societies centers of gravity include telecommunications networks, energy and power sources, transportation systems, and financial centers and networks. Thus, the destruction of these systems becomes just as important as destroying an adversary’s military forces. Not only will cyber-war be a force in future warfare, it may also turn out to be the great equalizer for nations attacking adversaries with superior conventional military power. Most nations lack the resources to build a military machine and may use information technologies to overcome their battlefield inferiority.” Id.

\(^{302}\) See Lynn, supra note 282, at 98.

\(^{303}\) Id. at 99.

\(^{304}\) See Susan Brenner & Leo L. Clarke, Civilians in Cyber warfare: Conscripts, 43 VAND. J. TRANSAT’L L. 1011, 1029 (2010) (civilians affect the defense of cyber warfare because they generally own and operate the nation’s critical infrastructure). Throughout history, warring nations have sought to demolish enemy critical infrastructure in order to cripple that nation. See Kamal, supra note 6, at 76 (“In previous wars, critical infrastructure components such as airports, power plants, water systems, railroads, oil and gas pipelines, and communication centers were targeted by the military because their destruction could help cripple a nation.”). This theory is founded on the principle that victory need only be achieved through attacking enemy infrastructure in conjunction with defeating its military forces. Id.
create a loss of confidence in the United States government and wreak economic havoc. These attacks deprive the victim state of its civilian infrastructure used to support military operations, such as electric power. Military dependence on civilian infrastructure has progressed to the point where victory in war can only be attained through the annihilation of the state itself, and the morale of its civilian population.

In review, states will use cyber warfare regardless of an international treaty prohibiting the use of cyber weapons. First, attributing responsibility for cyber attacks is problematic. Second, cyber warfare

---

305 See Brian M. Mazanec, The Art of (Cyber) War, 16 J. Int’l Sec. Aff. (2009), available at www.securityaffairs.org/issues/2009/16/mazanec.php. “Strategic cyber warfare attacks during a total war with the U.S. would destroy critical infrastructure and wreak economic havoc, but their most critical impact may be on the will of the U.S. population. By creating a chronic loss of services such as power, emergency response, television and telephony across the U.S., citizens would suffer a loss of confidence in the U.S. government. Individuals would question the status and security of their personal finances in savings and retirement accounts, and uncertainty could lead to rioting and hoarding that would act as a force multiplier, further stressing an already damaged infrastructure.” Id.

306 See Brenner & Leo L. Clarke, Civilians in Cyber warfare: Conscripts, 43 Vand. J. Transatl. L. 1011, 1029 (2010). For example, “coordinating the deployment and resupply of U.S. troops with goods from private vendors necessarily requires using unclassified networks that are linked to the open Internet.” See Lynn, supra note 282, at 100. Attacking these civilian networks could create large logistic problems for the United States in wartime. Id.

307 Kamal, supra note 6, at 78. (“In the late nineteenth century, military forces began to rely on industry for sustenance. This dependence has progressed to the point where wars are no longer aimed at defeating the enemy on the battlefield; they are wars of attrition, in which victory can be attained only through the destruction of the state itself, and the morale of its civilian population.”).

308 See supra Part III-B.

309 Id.
regulations cannot be realistically enforced. Third, the decentralized structure of the Internet fosters an environment of cyber exploitation. Fourth, most cyber attacks go unreported allowing cyber attacks to escape accountability. Fifth, the costs to operate in cyberspace are nominal. Sixth, cyber warfare can be used to circumvent traditional military forces. Seventh, cyber attacks can destroy a victim state’s internal operations viability. For the foregoing reasons, nations will use cyber warfare regardless of any international treaty.

V. PROPOSAL

The Federal government should protect critical infrastructure in the United States, because cyber threats towards critical infrastructure endangers national security. Civilian infrastructure in the United States supports the military in significant ways. They help provide power, telecommunications, and logistics. Unfortunately, the private sector is not able to provide adequate protections against major military attacks through cyberspace. The federal government needs to

310 Id.
311 Id.
312 Id.
313 Id.
314 Id.
315 Id.
316 Id.
317 See supra Part II.
319 Id.
be able to monitor the networks of these critical infrastructures in order to safeguard national security.

First, the federal government should implement active computer defenses to protect private sector critical infrastructure networks. The National Security Agency has created an advanced active cyber security defense system that can be applied to private critical infrastructure.321 These defense systems work by implementing scanning technology at the interface of military Internet networks to detect malicious code before it enters the network.322 These active defenses protect all networks under the “.mil” domain.323 Because active cyber security systems can prevent cyber attacks from entering targeted networks, the federal government should implement them on private critical infrastructure networks.

Second, the federal government needs to be able to regularly monitor critical infrastructure networks, because cyber defenses are not absolute.324 Some attacks will be able to infiltrate the networks and evade detection.325 This requires cyber warriors to be able to detect intruders and malicious code once it has been

321 See Lynn, supra note 282, at 103; see also Dep’t of Def., Dep’t of Def. Strategy for Operating in Cyberspace 7 (2011). “Active cyber defense is DOD’s synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DOD networks and systems, supplementing best practices with new operating concepts.” Id.

322 See Lynn, supra note 282, at 103; Strategy for Operating in Cyberspace, supra note 321, at 7 (active cyber defenses operate in real time “by using sensors, software, and intelligence to detect and stop malicious activity” before it can affect networks).

323 Lynn, supra note 282, at 103.

324 See Strategy for Operating in Cyberspace, supra note 321, at 7 (“[I]ntrusions may not always be stopped at the network boundary.”).

325 Lynn, supra note 282, at 103.
installed in the target network.\textsuperscript{326} Cyber warriors would need to be able to search through the private networks in order to hunt for malicious code and intrusions.\textsuperscript{327}

Active defense measures against United States private companies may infringe upon certain civil liberties enjoyed under the Constitution.\textsuperscript{328} Cyber warriors will have to search throughout private networks for intrusions. This raises concerns for private companies because of the expectation of privacy in their networks, and the sensitive proprietary information contained on it.\textsuperscript{329} “The law must therefore adjust traditional understandings of the right to privacy, the right to protection against an unreasonable search, and the right to due process.”\textsuperscript{330}

To preserve civil liberties, Congress should enact legislation that allows Cyber Command to monitor private networks upon judicial approval. Foremost, Congress should enact the Critical Infrastructure Cyberspace Surveillance Act (“CICSA”).\textsuperscript{331} Such an act would establish a CICSA Court.\textsuperscript{332} CICSA would authorize Cyber Command to electronically monitor private sector critical infrastructure networks for up to

\begin{footnotes}
\item[326] Id.
\item[327] Id.
\item[328] See Condron, supra note 221, at 416.
\item[329] U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347 (1967) (a search occurs when there is a reasonable expectation of privacy).
\item[330] See Condron, supra note 221, at 416.
\item[332] See e.g., Foreign Intelligence Surveillance Court Rules of Procedure 4, 5 (2006). The CICSA Court shall consist of United States District Court Judges appointed by the Chief Justice of the United States Supreme Court. Each Judge may exercise the authority vested by CICSA and such other authority as consistent with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.
\end{footnotes}
one year.\textsuperscript{333} In order to obtain authorization, Cyber Command would be required to show certain specific findings,\textsuperscript{334} and would obtain authorization only if approved through a CICSA Court judge.\textsuperscript{335} Cyber Command would then have the authority to only monitor private networks for malicious code. They would not have the authority delete malicious code from private networks. Instead, Cyber Command would be limited to acquire a court order forcing the private entity to fix their network vulnerabilities.

VI. CONCLUSION

To conclude, this article has demonstrated that: (1) nations around the world have militarized the power of cyberspace;\textsuperscript{336} (2) cyber warfare represents a serious threat to critical infrastructure within the United States.  

\textsuperscript{333} One year’s time may be needed in order to conduct a forensic computer investigation.

\textsuperscript{334} Each application for an order approving electronic surveillance under CICSA shall include:

(1) the identity of the Cyber Command officer making the application;

(2) the identity and description of the specific target of the electronic surveillance;

(3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—

(A) the target of the electronic surveillance is or has been the victim of cyber attacks within the past three years; and

(B) the cyber attacks were caused by a foreign nation or an agent of a foreign nation;

(4) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance.


\textsuperscript{335} For a judge to issue a surveillance order, probable cause must show that (1) the target of the surveillance has been the victim of cyber attack(s), and (2) the cyber attack(s) were caused by a foreign nation or an agent of a foreign nation.

\textsuperscript{336} \textit{See supra} Part I-C.
States;\footnote{See supra Part II.} and (3) international treaties do not provide adequate legal mechanisms to govern cyber warfare.\footnote{See supra Part III.} For the foregoing reasons, the United States should not depend on international legislation to protect its’ critical infrastructure from cyber attacks.\footnote{See supra Part IV.} Instead, the United States should take an active defensive approach, by monitoring the networks of private companies that own and maintain critical infrastructure within the United States.\footnote{Id.}
They Did It For The Lulz: Future Policy Considerations In The Wake Of Lulz Security And Other Hacker Groups’ Attacks On Stored Private Customer Data

By Jesse L. Noa*

“This is disgraceful and insecure: they were asking for it.” - Lulz Security

I. INTRODUCTION

The prevalence of companies storing private customer data has risen dramatically since the advent of the internet.1 This trend is illustrated by the fact that the amount of electronic data generated in 2011 was approximately 1.8 Zettabytes, or 1.8 trillion gigabytes.2 Among the data being generated and stored by companies is customers’ private information.3 This data includes social security numbers, credit card information, account numbers, birth dates, addresses,

* Jesse Noa is a 2013 J.D. Candidate of Villanova University School of Law; He holds a B.A. in Economics, Aug. 2009, summa cum laude, Rowan University.


3 See Rancourt, supra note 2, at 184-85 (discussing types of data typically stored by corporations).
emails, phone numbers, and other sensitive data that if misused, can destroy the finances of a person and potentially bring ruin to their lives.\textsuperscript{4} Due to the increase of stored private data, protecting customer information is becoming increasingly important.\textsuperscript{5} Failure to institute adequate protections for customer data has resulted in several class action lawsuits due to security breaches by hackers.\textsuperscript{6} These breaches have resulted in the loss of monumental amounts of customer data and the increased


\textsuperscript{5} See id. (estimating that each year over nine million Americans are victims of identity theft).

\textsuperscript{6} See e.g., Reilly v. Ceridian Corp., 664 F.3d 28, 40 (3d Cir. 2011) (suing for compromised data); Pisciotta v. Old Bat. Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (filing suit for lost customer data); Krotter v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010) (suing due to compromised customer data); Amburgy v. Express Scripts Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009) (filing suit as result of lost customer data); Hammond v. Bank of N.Y. Mellon Corp., No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307 *1-*2 (S.D.N.Y. June 25, 2010) (suing company due to customer data being compromised).

One such hacker group was Lulz Security which was a loosely organized group of hackers who specialized in attacking poorly protected websites. See Q&A: Lulz Security, BBC NEWS AND TECHNOLOGY (last updated June 26, 2011, 4:30 p.m.), available at http://www.bbc.co.uk/news/technology-13671195 (answering various questions regarding hacker group Lulz Security). The group existed for fifty days before disbanding and during their time attacked a wide range of targets such as Sony and the Central Intelligence Agency. Recently, several arrests of the members of the LulzSec have occurred as a result of the help of one of the leaders who began working with the FBI. See Jana Winter, EXCLUSIVE: Infamous International Hacking Group LulzSec Brought Down By Own Leader, FOXNEWS (Mar. 02, 2012), http://www.foxnews.com/scitech/2012/03/06/hacking-group-lulzsec-swept-up-by-law-enforcement/ (detailing how LulzSec’s leader helped FBI make major arrests through the organization).
This has been exemplified by the massive loss of private data by Sony at the hands of the hacker group Lulz Security and other hackers who exploited Sony’s almost nonexistent network security.\(^7\) Currently, companies have been shielded from liability for failure to protect the stored data through lackluster regulation on the state and federal levels as well as by burdens that plaintiffs must overcome in order to hold companies accountable in court.\(^9\) Although this is the current state of affairs, the tides may be changing as new laws emerge which may expose companies to liability for their failings.\(^10\)

This Comment explores the present state of private stored data, analyzing the current trends in the statutory and common law, and offers policy considerations for companies looking to avoid the explicit and implicit costs of a data breach. Part II outlines the significance of customer data protection in the digital age. Part III discusses the massive data breach at Sony, analyzing its legal and financial significance for corporate protection of customer data. Part IV provides an overview of other significant data breaches and their impacts. Part V examines the hurdles plaintiffs face when bringing claims against companies for inadequate data protection. Additionally, Part V discusses current state and federal laws, focusing on

---

\(^7\) See Rancourt, supra note 1 at 185 (noting that Sony PlayStation network breach affected over seventy million customers and in TD Ameritrade’s breach, over 6.3 million customers were affected).

\(^8\) For a discussion regarding the Sony data breaches, see infra notes 25-91 and accompanying text.

\(^9\) For a discussion regarding the legal burdens which plaintiffs have yet to overcome in bringing data breach claims against companies, see infra notes 127-199 and accompanying text.

\(^10\) For a discussion regarding the developing case and statutory law in the area of data breaches and company network security, see infra notes 127-199 and accompanying text.
their shortcomings. Finally, Part VI highlights several policy and financial considerations that companies should be mindful of in developing their network security and suggests guidelines companies should follow in the future.

II. THE CURRENT STATE OF PRIVATE STORED DATA

With the advent of the technological revolution, companies have increasingly used the internet as a means of conducting business.\textsuperscript{11} As more commerce is conducted online, whether through direct sales, account memberships, online gaming, blogs, or other means, a staggering amount of customer data is being processed and stored on the internet.\textsuperscript{12} As of 2011, the total amount of online stored data is estimated to be 295 exabytes, or 295 billion gigabytes.\textsuperscript{13} To put this into perspective, on a single day American businesses generate more data than what “exist[s] in every book in every library in America.”\textsuperscript{14}

\textsuperscript{11} See Timothy H. Madden, \textit{Data Breach Class Action Litigation - A Tough Road for Plaintiffs}, 55 BOSTON B.J. 27, 27-28 (Fall 2011) (noting increased use of electronic methods of conducting business and greater need to transmit and store sensitive information).

\textsuperscript{12} See Suzanne Wu, \textit{How Much Information is There in the World?}, UNIV. SO. CAL. NEWS (Feb 10, 2011), available at http://uscnews.usc.edu/science_technology/how_much_information_is_there_in_the_world.html (discussing massive amount of information created and stored).

\textsuperscript{13} See Lucas Mearian, \textit{Scientists Calculate Total Data Stored to Date: 295+ Exabytes}, COMPUTERWORLD (Feb. 14, 2011), available at http://www.computerworld.com/s/article/9209158/Scientists_calculate_total_data_stored_to_date_295_exabytes (discussing recent study which calculated amount of data stored online).

As a result of the increased use of the internet as a means of commerce, consumers have had to adapt to a world where hackers can steal their identities, their banking and credit card information, as well as other types of personal data.\textsuperscript{15} Hackers typically do this in order to steal money and make purchases under false identities, for activist reasons, or just for the fun of it.\textsuperscript{16} Because of these risks, customers need to be assured that their personal data is protected.\textsuperscript{17} Problems arise when companies storing personal data about their customers on online networks fail to enact appropriate security controls and procedures to ensure that the stored data is not compromised.\textsuperscript{18} Due to the prevalence of the internet as a means for doing business, it is almost impossible for customers to avoid having their personal data stored by at least some companies.\textsuperscript{19} When companies fail to adequately protect such data, customers become vulnerable to having their personal information used against them and are helpless to

\begin{footnotesize}
\footnotesize
\textsuperscript{15} See \textit{About Identity Theft}, supra note 4 (discussing types of information identity thieves steal and how they do so).
\textsuperscript{16} See id. (noting hackers and thieves stealing identities to profit from victims). \textit{See also} Kevin Komiega, \textit{Political Hacking: Crime or Activism?} \textsc{Search Security} (Dec. 13, 2000), http://searchsecurity.techtarget.com/news/506135/Political-hacking-Crime-or-activism (discussing use of hacking and other electronic methods as form of political activism).
\textsuperscript{17} See Fahmida Y. Rashid, \textit{Fixing Data Breaches: Tracking the Cost and Damage Toll}, \textsc{EWeek} (Mar. 14, 2011), http://mobile.eweek.com/c/a/Security/Fixing-Data-Breaches-Tracking-the-Cost-and-Damage-Toll-605411/ (noting increasing mistrust customers have regarding data breaches and customers leaving companies due to data breaches).
\textsuperscript{18} For a discussion regarding the storage of data and the effects of a company not adequately protecting that data, see infra notes 119-126, 200-217 and accompanying text.
\textsuperscript{19} See Madden \textit{supra} note 12 at 27 (discussing increased use of e-commerce in day to day life).
\end{footnotesize}
prevent it, possibly to their financial detriment.\(^{20}\) For example, in 2011 nearly twelve million Americans were victims of identity theft.\(^{21}\) That same year, as a result of data breaches similar to the ones that occurred at Sony, the number of people whose personal information was stolen increased by sixty-seven percent.\(^{22}\)

Companies who store their customers’ data on online networks and databases should be considered to have taken on the duty to appropriately and adequately protect that data from theft and misuse.\(^{23}\) Online attacks on company networks, facilitated by inadequate protection of customer data, can lead not only to potential legal liability but also to the alienation of customers, plummeting stock prices, loss of market share, and the financial ruin of customers whose identities have been stolen.\(^{24}\)


\(^{22}\) See id. (discussing Sony’s and other high profile data breaches’ role in the increased proliferation of private customer data in the hands of hackers). For a discussion regarding the Sony and other data breaches, see infra notes 25-126 and accompanying text.

\(^{23}\) For a discussion regarding companies storing customer data, the effects of not adequately protecting it, and policy considerations, see infra notes 25-126, 200-232 and accompanying text.

\(^{24}\) For a discussion regarding the Sony data breaches and the effects on the company and its customers, see infra notes 25-91 and accompanying text.
III. THE “SOWNAGE CAMPAIGN”: THE TOTAL DECIMATION OF SONY’S ONLINE NETWORKS

A. SOWNAGE: HOW HACKERS BROUGHT SONY TO ITS KNEES IN TWO MONTHS

Last year Sony was exposed for having inadequate network protection of their customer data through many uncoordinated attacks against both its PlayStation networks and its entertainment divisions.25 The first attack was on April 04, 2011, by the activist hacker group Anonymous.26 Anonymous attacked Sony’s PlayStation Network (“PSN”) with a Denial of Service attack (“DOS”) in retaliation for Sony’s lawsuit against George Hotz; better known in the online

---

25 See Absolute Sownage: A Concise History of Recent Sony Hacks, ATTRITION (Last Updated June 4, 2011), http://attrition.org/security/rant/sony_aka_sownage.html (detailing hacks by various groups against all parts of Sony’s business).

26 See id. (detailing timeline of Sony’s security breaches).
community as ‘GeoHot’. 27 Although the DOS attack created a nuisance for Sony and its users, it did not compromise customer data. Following Anonymous'

27 See id. (noting Anonymous declared war on Sony, attacking PlayStation Network in retaliation for Sony’s lawsuit against GeoHot). The ‘GeoHot’ lawsuit involved Sony suing George Hotz for jailbreaking the Sony PlayStation 3 (“PS3”). See Audrey Watters, Sony and “GeoHot” Settle PS3 Jailbreak Lawsuit, READWRITEWEB (Apr 11, 2011), http://www.readwriteweb.com/archives/sony_and_geohot_settle_ps3_jailbreak_lawsuit.php (discussing Sony’s settlement with George Hotz as well as details of lawsuit). Sony claimed that jailbreaking the PS3 allowed users to play pirated i.e., illegally obtained versions of the games on the PS3. See id. Sony also claimed that by jailbreaking the PS3, George Hotz breached the Digital Millennium Copyright Act as well as the Computer Fraud Abuse Act. See id. Jailbreaking involves hacking or modifying the game console in order to give the user access to the code of the gaming console. See Roydon Cerejo, PS3 Jailbreaking: Is it Worth it?, TECHTREE (Mar 28, 2011), http://www.techtree.com/India/Features/PS3_Jailbreaking_Is_it_Worth_it/551-114940-899.html (discussing what jailbreaking is as well as pros and cons for jailbreaking PS3). Anonymous “is not an organized collective of like-minded hackers. Rather, it’s a banner that many different hacktivist groups rally behind in an attempt to gather enough support to take down an opponent.” See David Goldman, Hacker Group Anonymous a Nuisance, Not a Threat, CNN MONEY (January 20, 2012), available at http://money.cnn.com/2012/01/20/technology/anonymous_hack/index.htm (detailing Anonymous as loosely affiliated activist hacker group). The actions of Anonymous are typically in the form of online protests to certain events such as the attack on Wall Street websites and systems in support of the Occupy Wall Street movement as well as attacks on the CIA, FBI, and entertainment websites in protest of the Stop Online Piracy Act (“SOPA”). See id. A DOS attack is where a hacker “attempts to prevent legitimate users from accessing information or services.” See National Cyber Alert System, Cyber Security Tip ST04-015: Understanding Denial-Of-Service Attacks, U.S. COMPUTER EMERGENCY READINESS TEAM (Last Updated Nov. 4, 2009), available at http://www.us-cert.gov/cas/tips/ST04-015.html (detailing what DOS attack does to networks). Essentially, a DOS attack creates a flood of traffic to the target network, which overloads the servers, causing the network to go offline; preventing users’ ability to access the network. See id.
attack on the PSN, a more substantial offensive was launched.\textsuperscript{28}

On April 19, 2011, Sony became aware that the PSN was compromised and began investigating the source and effect of the breach but did not alert its users.\textsuperscript{29} The next day on April 20, 2011, Sony took the PSN offline in response to the breach.\textsuperscript{30} Despite this action, Sony did not publicly acknowledge that they knew of a data breach, but stated that, “[w]e’re aware certain functions of the PlayStation Network are down. We will report back here as soon as we can with more information.”\textsuperscript{31} Additionally, Sony hired an outside security company to work on the PSN.\textsuperscript{32} On April 21, 2011, Sony asserted that the PSN would be back online in a matter of days.\textsuperscript{33} Further, Sony remained silent on the fact that PSN suffered a data breach even though numerous blogs and gaming news sites began questioning the possibility.\textsuperscript{34} On April 22, 2011, Sony finally declared that an external breach was the cause of PSN being taken offline, stating, “[a]n external intrusion

\textsuperscript{28} See Absolute Sownage, supra note 25 (detailing further hacks against Sony’s network systems).


\textsuperscript{30} See id. (noting Sony’s choice to take PSN offline in response to data breach).

\textsuperscript{31} See id. (discussing Sony’s failure to inform public of data breach).

\textsuperscript{32} See id. (noting Sony’s decision to bring in outside security company to work on data breach investigation).

\textsuperscript{33} See id. (observing that Sony claimed PSN would be back online within “a full day or two.”).

\textsuperscript{34} See id. (noting that several gaming related sources and blogs began reporting on possibility of a data breach being cause of PSN going offline).
on our system has affected our PlayStation Network and Qriocity services. In order to conduct a thorough investigation and to verify the smooth and secure operation of our network services going forward, we turned off PlayStation Network & Qriocity services.\textsuperscript{35} Although Anonymous took responsibility for DOS attacks on the PSN in response to the GeoHot lawsuit, the group claimed that, as a whole, they were not responsible for the breach.\textsuperscript{36} Additionally, Anonymous, as part of their denial of being the cause of the outage, hinted at the PSN security measures being fatally flawed.\textsuperscript{37}

On April 23, 2011, Sony indirectly acknowledged the severity of the breach and inadequacy of its network security by stating that the PSN needed to remain offline to rebuild the entire system.\textsuperscript{38} Sony gave no timeline of when they expected the PSN to be back

\textsuperscript{35}See id. (discussing Sony’s convoluted disclosure regarding external intrusion of PSN).

\textsuperscript{36}See id. (noting that Anonymous claimed group was not responsible but that individual members may have acted against PSN.) See also Sara Yin, ‘Anonymous’ to Sony: For Once We Didn’t do it, PC MAGAZINE (Apr. 22, 2011), available at http://www.pcmag.com/article2/0,2817,2384012,00.asp (discussing Anonymous’s denial that they caused PSN’s outage).

\textsuperscript{37}See Yin, supra note 36 (quoting Anonymous that Sony was attempting to blame PSN outage on Anonymous rather than fact PSN having internal problems). As part of their denial for the outage, Anonymous stated,

[w]hile it could be the case that other Anons have acted by themselves AnonOps was not related to this incident and takes no responsibility for it. A more likely explanation is that Sony is taking advantage of Anonymous’ previous ill-will towards the company to distract users from the fact the outage is actually an internal problem with the companies servers.

See id.

\textsuperscript{38}See Williams, supra note 29 (discussing Sony’s disclosure of fact that PSN network needed to be rebuilt as result of attack).
online. On April 24, 2011, Sony hired a second outside security company to help work on the data breach, further highlighting the depth of the problem. On April 25, 2011, although the outside security companies had concluded that the data breach resulted in customer data being compromised, Sony explicitly and publicly stated that such determination had not yet been made. On April 26, 2011, the head of Sony’s gaming division, Kaz Hirai, held a news conference in Tokyo and discussed the unveiling of the company’s new tablet computers but did not discuss the PSN breach. Later on that same day, Sony released a statement regarding the PSN breach. At that point, Sony finally admitted that customer data was stolen as a result of the breach. Sony stated that:

[W]e believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address (city,

39 See id. (noting that there was no timeline of when PSN may be put back online).
40 See id. (discussing Sony’s hiring of second outside security company to work on PSN).
41 See id. (noting security companies had discovered that customer data had been compromised as part of breach even though Sony publicly stated it was unsure if data had been breached and that Sony would notify consumers promptly if it was clear “personal information or credit card numbers of users had been compromised. . .”).
42 See id. (discussing Mr. Hirai’s decision not to take questions after conference and his failure to discuss PSN breach).
43 See id. (noting that Sony gave its most detailed release regarding breach).
state, zip), and your PlayStation Network/Qriocity password security answers may have been obtained. If you have authorized a sub-account for your dependent, the same data with respect to your dependent may have been obtained. While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility. If you have provided your credit card data through PlayStation Network or Qriocity, out of an abundance of caution we are advising you that your credit card number (excluding security code) and expiration date may have been obtained.\footnote{See Patrick Seybold, \textit{Update on PlayStation Network and Qriocity}, PLAYSTATION.BLOG (Apr. 26, 2011), http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/ (detailing official Sony statement regarding amount and type of data stolen as result of breach of PSN).}

The number of users affected by the breach was approximately seventy-seven million.\footnote{See \textit{Absolute Sownage}, supra note 25 (detailing number of users who had their data compromised).} The day after Sony made their public statement, a class action lawsuit was filed, alleging that Sony failed to take "reasonable care to protect, encrypt and secure the private and sensitive data of its users."\footnote{See Williams, supra note 29 (discussing pending class action lawsuit filed against Sony as result of inadequate network security and subsequent breach of PSN and Qriocity).} Encryption is the use of sophisticated algorithms to convert the data into ‘ciphertext’ which cannot be easily understood without a key or the correct decryption technology, making it much more difficult to glean meaningful information unless having such tools. \textit{See} Robert Bauchle, Fred Hazen, John Lund, Gabe Oakley, & Frank Rundatz, \textit{Encryption}, SEARCH SECURITY (last updated July 2006), http://searchsecurity.techtarget.com/definition/encryption (defining encryption).
lies with the executives who declared a war on hackers, laughed at the idea of people penetrating the fortress that once was Sony, whined incessantly about piracy, and kept hiring more lawyers when they really needed to hire good security experts. . . .”

Additionally, a congressional committee contacted Sony asking them to explain and detail the massive data breach. Finally, after being offline for twenty-five days, Sony reactivated the PSN.

In addition to their problems with the PSN/Qriocity, other areas of Sony’s business networks were being attacked. On May 2, 2011, Sony shut down its Sony Online Entertainment Service (“SOES”) after it was hacked. As a result of the hack, Sony stated that it believed more than 23,000 customers’ credit card and banking data may have been stolen. It was also confirmed that hackers gained access to 24.6 million SOES users’ personal information, similar to what was

47 See Williams, supra note 29 (quoting George Hotz who claimed breach was in response to Sony’s arrogance regarding network security and Sony’s treatment of hacker and online community).

48 See id. (noting U.S. congressional committee’s contact with Sony).


50 See Absolute Sownage, supra note 25 (outlining numerous attacks on all aspects of Sony’s business).

51 See Robert McMillan, Sony Cuts Off Sony Online Entertainment Service After Hack, COMPUTERWORLD (May 2, 2011), available at http://www.computerworld.com/s/article/9216343/Sony_cuts_off_Sony_Online_Entertainment_service_after_hack (discussing Sony’s decision to shutdown SOES after Sony discovered it was also hacked in addition to PSN). The SOES is a gaming network use for massive multiplayer online games (“MMOG”). See id.

52 See id. (discussing data stolen as result of breach of SOES).
stolen through the attack on the PSN. Additionally, as part of the hack on the SOES network, Sony stated that the hackers gained access to an outdated database which contained “card numbers and expiration dates for 12,700 customers based outside of the U.S., and direct withdrawal data belonging to some customers in Austria, Germany, the Netherlands and Spain.”

Sony’s networks were again attacked on May 23, 2011, when the hacker group Lulz Security breached Sony Music Japan (“SMJ”) through a simple Structured Query Language (“SQL”) injection. A SQL injection

---

53 See Liana B. Backer & Jim Finkle, Sony Hires Firm to Clean Up After Breach, REUTERS (May 3, 2011), available at http://www.reuters.com/article/2011/05/03/us-sony-idUSTRE73R0Q320110503. (noting personal information such as names, email addresses, and passwords were also stolen as a result of SOES breach).

54 See McMillan, supra note 51. (noting hackers ability to gain access to database with sensitive customer information).

is a simple intrusion method that tricks a website and database into running codes that are not intended by the owner of the website/database. Not only did Lulz Security breach SMJ, but they widely publicized the stolen information across the internet. Luckily for customers of SMJ, Lulz Security was not a malevolent hacker group, but rather an activist group, and

A SQL injection attack is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a Web application for execution by a backend database. Attackers take advantage of the fact that programmers often chain together SQL commands with user-provided parameters, and can therefore embed SQL commands inside these parameters. The result is that the attacker can execute arbitrary SQL queries and/or commands on the backend database server through the Web application. See SQL Injection, IMPERVA (last visited Jan. 31, 2013), http://www.imperva.com/resources/glossary/sql_injection.html (describing SQL injection attack). SQL has become very prevalent in web applications due to the use of databases to store and process information. See SQL (Structured Query Language), NTC HOSTING (last visited Jan. 31, 2013), http://www.ntchosting.com/databases/structured-query-language.html (detailing SQL and its importance in maintaining and rationalizing information stored on online databases). “SQL is responsible for querying and editing information stored in a certain database management system.” Id.


See Winniewski, supra note 55 (discussing Lulz Security’s publication of stolen user data from hack of SMJ).
accordingly did not publish sensitive data such as credit card or banking information.\textsuperscript{58}

Sony’s network problems continued as the Lebanese hacker known as “Idahc” breached Sony Ericsson through a SQL injection on the same day Lulz Security hacked SMJ.\textsuperscript{59} The hack resulted in over 1,000 customers having their personal data compromised.\textsuperscript{60} Similar to Lulz Security, Idahc published the stolen data online for anyone on the web to see.\textsuperscript{61}

In response to these attacks, Sony should have changed its network protections or control systems or at the very least encrypted their customer data. Instead, on June 2, 2011, Lulz Security scored another massive breach on Sony Pictures, stealing over one million user logins as well as addresses and birthdates.\textsuperscript{62} This time, Lulz Security did not hack for the ‘lolz’ but rather to teach a lesson, stating:

\textsuperscript{58} \textit{See id.} (noting Lulz Security did not publish banking or credit card information after hack of SMJ).


\textsuperscript{61} \textit{See id.} (noting Idahc’s publishing of compromised customer data).

\textsuperscript{62} \textit{See} Sam Biddle, \textit{Hackers Spill Over 1,000,000 Sony Pictures Online Accounts}, \textit{GIZMODO} (June 2, 2011), http://gizmodo.com/5807996/hackers-spill-over-1000000-sony-online-accounts (discussing Lulz Security’s hack on Sony Pictures and subsequent release of customer data to the internet).
[o]ur goal here [was] not to come across as master hackers, hence what we’re about to reveal: SonyPictures.com was owned by a very simple SQL injection, one of the most primitive and common vulnerabilities, as we should all know by now. From a single injection, we accessed EVERYTHING. Why do you put such faith in a company that allows itself to become open to these simple attacks?\textsuperscript{63}

The hack by Lulz Security revealed that accessing the data was a simple matter, and showed that the customer data was stored in plain text rather than being encrypted, which rendered the information practically defenseless against malevolent hackers.\textsuperscript{64} Lulz Security continued to attack Sony’s networks and on the same day as the Sony Pictures hack, they breached Sony Bertelsmann Music Group (“BMG”) and publicly posted Sony’s developer source code as well as Sony BMG’s network maps.\textsuperscript{65}

\textsuperscript{63} See id. (noting Lulz Security’s explanation for hacking and releasing Sony Pictures customer data) (emphasis in original).

\textsuperscript{64} See id. (discussing Sony’s complete failure to protect their customers’ data from hackers).

Sony’s problems continued on June 20, 2011, when hackers Idahc and Auth3ntiq gained access to 177,000 emails from Sony Pictures France. Yet again, one of Sony’s networks was breached through a simple SQL injection. Fortunately for the users of Sony Pictures France, the hacking duo did not publish their user information on the internet. According to Idahc, he breached Sony Pictures France to prompt Sony to improve their security. With the addition to Idahc and Auth3ntiq’s hack on Sony Pictures France, the number of successful breaches of Sony’s networks reached twenty in a matter of two months.

The sheer number of successful breaches of Sony’s networks showed that despite taking several of its networks offline in response to the initial security breaches, Sony had failed to fix the fundamental security

67 See id. (discussing method used to hack into Sony Pictures France). The SQL injection method had been used previously as discussed above to steal user information from Sony Music Entertainment Japan, SonyPictures.com and Sony Pictures Russia. See id.
68 See id. (noting that hackers did not publicly publish compromised user data).
69 See id. (discussing Idahc’s interview with Forbes Magazine in which Idahc claimed the hack was for purpose of motivating Sony to improve its network security).
70 See id. (noting number of recent hacks of Sony’s networks after initial PSN data breach).
problems of its networks.\textsuperscript{71} Furthermore, the success of these attacks demonstrated Sony’s complete failure to adequately secure their networks in the first place.\textsuperscript{72} These attacks drew attention to the corporation’s ignorance, apathy, or arrogance in not properly protecting the customer data stored on their networks.\textsuperscript{73}

The widespread significance of the attacks on Sony’s network is underscored not only by the company’s potential legal liability, but various other negative consequences Sony experiences due to their failure to adequately protect their customers’ data. The breach caused severe alienation among Sony’s customer base and created a lack of trust in what was once a pristine name brand corporation.\textsuperscript{74} This lack of trust can result in a massive loss in market share for Sony and


\textsuperscript{72} See Absolute Sownage, supra note 25 (noting the preposterousness of even debating whether attacks on Sony were advanced, stating that Sony failed to “implement[] what any rational administrator or security profession would consider ‘the basics.’ Storing millions of customer’s personal details and passwords without using any form of encryption is reckless and ridiculous.”).

\textsuperscript{73} See id. (discussing the reckless lack of security of Sony’s data networks).

companies like it. Further, such disregard to protecting customer data can lead to substantial losses in company value and drop in stock prices. These results are important for any company storing customer data to consider when deciding on policies and procedures for protecting such data.

B. SETTING SAIL FOR FAIL: HOW SONY’S INADEQUATE NETWORK SECURITY INVITED THE SOWNAGE CAMPAIGN

Where did Sony go wrong? Why was Sony targeted and attacked so many times? The answers lie in the statements of Lulz Security and Idahec who attacked Sony’s networks: it was done not only for the fun of it, but to show the public that a major corporation which was supposed to keep customer data private and protected, essentially left the door open to anyone who wanted to steal the information.

75 See Rashid, supra note 17 (discussing large costs associated with data breaches and how it drives costumers away from companies).


77 See Julianne Pepiton, Group Claims Fresh Hacks of 1 Million Sony Accounts, CNN MONEY (June 2, 2011), http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/index.htm (noting that Lulz Security stated “Sony was ‘asking for it’ by storing more than 1 million user passwords in plain text, instead of encrypting them.”). Lulz Security also stated that the level of security maintained by Sony was “disgraceful.” See id.
Sony’s major mistake was having little to no security for its stored data in the first place. Simple SQL injections should not be able to affect the databases of multi-billion dollar corporations and could have been avoided with simple security procedures. Furthermore, Sony failed to encrypt its users’ data. It could be argued that such encryption is unnecessary for easily accessible public information, but birthdates, account information, credit card numbers, and other financially sensitive information should be encrypted in order to protect against potentially devastating fraud and identity theft.

Another glaring issue regarding the data breaches was how Sony addressed it with the public. Sony waited one week after the discovery of the breach to notify its customers that their data had been

---

78 See Absolute Sownage, supra note 25 (noting that “Sony has demonstrated they have not implemented what any rational administrator or security professional would consider ‘the absolute basics.’”).

79 See Shaul, supra note 56 (discussing ease for hackers to use SQL injection attack and lack of difficulty to protect against such attacks with simple security procedures and vigilance).


81 See id. (noting that even though Sony encrypted credit card information, Sony failed to disclose what type of encryption was used and if it was adequate). Why Sony did not encrypt the user account information has been the topic of expert and political discussions since the breach. See id.

82 See Davey Winder, Where Hacked Sony Went Wrong, and LastPass Got it Right, PCPro (May 6, 2011), http://www.pcpro.co.uk/blogs/2011/05/06/where-hacked-sony-went-wrong-and-lastpass-got-it-right/ (discussing Sony’s response to the data breaches).
compromised. In the fast-paced computing world, such a slow response is unacceptable and reckless. Hackers had a week to launch any fraud or identity theft campaigns they wanted without Sony’s customers having any warning or ability to take the appropriate actions to protect themselves. As one of the largest entertainment companies in the world, such a delayed response is unacceptable not only from a customer standpoint but from a financial and managerial point of view.

Sony’s failings not only put their customers at risk but also created severe financial ramifications for the company. For example, the PSN was taken offline for twenty-five days, which prevented users from playing online, purchasing games, movies, or other services from Sony. The outage was estimated to cost Sony ten million dollars per week. The total estimated

83 See id. (discussing Sony’s delayed response in notifying its customer base of data breach).
84 See id. (noting how exposed customers became within one week).
85 See id. (detailing customers inability to take steps to protect themselves due to lack of notice).
86 See id. (implying that company of Sony’s size should have responded quicker to the issue and claiming such response was “[s]imply not good enough”).
87 For a discussion regarding the potential financial ramifications of a data breach, see infra notes 119-126, 200-217 and accompanying text.
88 See Hill, supra note 50 (discussing PSN coming back online). The PSN allows users to play online with other PlayStation users, as well as rent or buy movies, video games, and other services. See PlayStation®3 Features, PLAYSTATION (last visited Mar. 11, 2012), http://us.playstation.com/ps3/features/ps3featuresnetwork.html (describing features of PlayStation and PSN).
cost of the breach as well as the steps Sony took to remedy it was approximately $171 million.\textsuperscript{90} Furthermore, Sony’s actions breached its customers’ trust which may prevent future sales as well as drive customers to competitors.\textsuperscript{91} These negative consequences can be felt by any company that fails to institute adequate safeguards for consumer data stored online.

IV. OTHER NOTABLE DATA BREACHES

Sony was not the only company in recent years to have their databases breached by hackers.\textsuperscript{92} Many large companies, particularly in the finance industry, have been the focus of hacker attacks.\textsuperscript{93} Below is a short description of data breaches that have occurred at some major companies over the past few years, which further demonstrates the significant impact inadequate data protection can have on corporations and consumers.


\textsuperscript{91} See Pharm, \textit{supra} note 89 (noting PSN customer who stated “I doubt I will ever put my credit card information on their network again.”).


\textsuperscript{93} See Victoria McGrane & Randall Smith, \textit{Hacking at Citi is Latest Data Scare}, \textit{Wall Street Journal} (June 9, 2011), available at http://online.wsj.com/article/SB10001424052702304778304576375911873193624.html (noting that security experts claim financial institutions are “top target[s] for cybercriminals”). The security experts further noted that “[t]he most sophisticated hackers in the world target banks, and they target government agencies. . . .” See id.
A. CITIGROUP

In June of 2011, Citigroup was the focus of a major data breach that resulted in the compromise of over 360,000 customers’ data. The stolen information included names, addresses and account numbers. Citigroup’s response was to inform their customers within two weeks of discovering the breach and replacing the majority of their affected customers’ credit cards. Unlike the Sony breaches, the breach at Citigroup was the result of sophisticated hacking methods which involved an automated tool that repeatedly typed account numbers into the browser address bar in order to access the information.

B. RSA SECURITY

In March of 2011, alarms around the world went off when the premier computer security company, RSA Security (“RSA”), was hacked. This data breach was of significant importance because of the widely held view that if RSA could be hacked, then any company could be. The information stolen involved RSA’s SecurID products which provide additional protection to

---

94 See Kim Zetter, Citi Credit Card Hack Bigger Than Originally Disclosed, WIRED (June 16, 2011), available at http://www.wired.com/threatlevel/2011/06/citibank-hacked/ (discussing disclosure of increased number of accounts which had been compromised at Citigroup, bringing number from 200,000 to 360,000).
95 See McGrane, supra note 93 (detailing type of data stolen in hack of Citigroup).
96 See id. (discussing Citigroup’s response to the data breach).
97 See Zetter, supra note 94 (discussing method used by hackers to gain access to Citigroup’s customer account data).
99 See McGrane, supra note 93 (noting that “RSA ‘is like Fort Knox. If RSA can get hacked, anybody can get hacked.’”).
the user login process by “requiring users to enter a secret code number displayed on a key fob, or in software, in addition to their password.”100 This is important because over 250 million RSA customers use SecurID, which could potentially expose them to hacker attacks.101

Unlike the instances at Sony, which practically left the virtual door open, the hack at RSA involved a sophisticated three stage attack.102 The first stage involved sending phishing emails to small groups of employees, one of whom opened the email which contained malware.103 The malware exploited “a previously unknown flaw in Adobe’s Flash software

100 See Zetter, supra note 98 (detailing type of data stolen and what SecurID involves). SecurID is a two-factor authentication technology which creates an extra layer of protection over a simple password login. See id.

101 See id. (discussing effect breach of RSA may have on customers who use SecurID technology).

102 See Riva Richmond, The RSA Hack: How They Did it, N.Y. TIMES (April 2, 2011), available at http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/ (detailing how sophisticated attack on RSA was accomplished). See also Absolute Sownage, supra note 25 (noting “the attacks on Sony are not coordinated, nor are they advanced.”).

103 See Richmond, supra note 102 (discussing initial step hacker used to gain access to RSA system). The initial attack was successful when a single employee took the email out of the spam folder and opened the attached excel file. See id. Phishing “is a fraudulent attempt, usually made through email, to steal [someone’s] personal information. . . . Phishing emails usually appear to come from a well-known organization and ask for your personal information—such as credit card number, social security number, account number or password.” See What is Phishing, PHISHTANK (last visited Feb. 16, 2012), http://www.phishtank.com/what_is_phishing.php (defining phishing scam). Scammers will use emails with legitimate sounding titles and themes to try and coax potential victims into giving them their personal information. See id. The scammers later use that information to steal the victim’s identity and money. See id.
[allowing it] to install a backdoor.”\textsuperscript{104} With the backdoor in place, the hacker was able to steal passwords of that employee, enabling the hacker to gain access to other systems and other employees.\textsuperscript{105} After gaining access to the target files, the hacker sent the data to “a hacked machine at a hosting provider, and then on to the hacker himself.”\textsuperscript{106}

\textbf{C. LOCKHEED MARTIN}

The far reaching implications of the RSA security breach were seen when the information stolen from RSA was later used to gain access to the data of Lockheed Martin (“Lockheed”) at its main database center in Maryland.\textsuperscript{107} Hackers used “falsified SecurID electronic tokens to gain access” to Lockheed’s databases.\textsuperscript{108} Fortunately, Lockheed had broader

\begin{flushright}
\textsuperscript{104} See id. (explaining how malware was able to give hacker control over RSA employee’s computer). A backdoor program “allows the hacker to access [a] computer whenever it’s on the [i]nternet. It’s a remote control, and usually a very thorough one with full access to every facility and file on [a] computer.” See What Hackers Do, TiNHAT (last visited Mar. 11, 2012), http://www.tinhat.com/hackers/hacking.html.

\textsuperscript{105} See Richmond, supra note 102 (detailing how hacker was able to use employee’s computer and passwords to gain access to other parts of RSA, enabling hacker to gain access to sensitive data).

\textsuperscript{106} See id. (describing how hacker was able to transmit stolen data from RSA to controlled computer). The hacker left very few clues behind other than three Web addresses, one of which indicated a possible connection with the People’s Republic of China. See id.


\textsuperscript{108} See Kwame Opam, Lockheed Martin’s Security Networks, GIZMODO (May 28, 2011), http://gizmodo.com/5806485/lockheed-martins-security-networks-were-hacked (noting how hackers were able to gain access to Lockheed’s networks).
security systems which were able to lessen the effectiveness of the hackers’ attack.\(^{109}\) Accordingly, Lockheed was able to quickly discover the attack and minimize the areas affected by the breach.\(^{110}\) As a result of its quick actions, Lockheed stated that there was “no compromise of customer, program or employees’ personal data. . . .”\(^{111}\) Although Lockheed claimed that no sensitive data was compromised, the very fact that hackers may have been able to gain access to classified United States military research and defense files underscores the stakes involved with protecting stored data.\(^{112}\)

D. BANK OF AMERICA

The financial costs of a data breach were illustrated when Bank of America suffered a data breach which allowed hackers to steal “at least $10 million from the bank.”\(^{113}\) This breach was not the result of a highly sophisticated hack, as was the case in the RSA breach, but rather by a low tech method; an insider leaked

\(^{109}\) See id. (stating that Lockheed’s broader security measures helped “soften the blow” from the breach).

\(^{110}\) See Mick, supra note 107 (noting that Lockheed “detected the [hack] ‘almost immediately’ and warded it off quickly.”).

\(^{111}\) See id. (noting Lockheed’s claim that breach on their network did not compromise secured data).

\(^{112}\) See id. (detailing some of stored data as relating to “the F-16, F-22 and F-35 fighter aircraft; the Aegis naval combat system; and the THAAD missile defense.”).

confidential information to scammers and hackers.\textsuperscript{114} The information leaked included names, addresses, social security numbers, bank account numbers, birthdates, drivers’ licenses, and more.\textsuperscript{115} This information gave the scammers the ability to fraudulently withdraw money from the customers of Bank of America.\textsuperscript{116} The ability for an employee to steal and leak customer information so easily shows a flaw in Bank of America’s data protection policy. This was especially apparent because Bank of America had stated it was going to strengthen its data security due to threats from Wikileaks regarding the release of “damaging

\textsuperscript{114} See David Lazarus, \textit{Bank Of American Data Leak Destroys Trust}, \textit{LA TIMES} (May 24, 2011), available at http://articles.latimes.com/2011/may/24/business/la-fi-lazarus-20110524 (detailing how customer data was leaked to scammers by former employee). The leaked data was later used to fraudulently withdraw funds from customer accounts. See id. Bank of America is not the only company to lose the sensitive data of their customers through very low-tech means. British Petroleum (“BP”) recently lost the personal data of over 13,000 people who had filed claims against BP as a result of the Gulf oil spill simply because a BP employee lost the laptop containing the information. See Associated Press, \textit{BP Loses Laptop With Gulf Residents’ Claim Data}, \textit{CBS NEWS} (Mar. 29, 2011), http://www.cbsnews.com/stories/2011/03/29/business/main20048504.shtml.

\textsuperscript{115} See Lazarus, \textit{supra} note 115 (listing type of customer data leaked to scammers).

\textsuperscript{116} See id. (discussing how hackers were able to withdraw money from customer accounts using Andrew Goldstein, Bank of America Customer, as example). Not only were the scammers able to use the stolen data to get checks, but they also contacted Bank of America’s customer service to successful transfer funds from non-compromised accounts to compromised ones. See id.
information.”117 As a result of the leak, Bank of America has had to reimburse its customers who had their money stolen as well as provide two years of free credit monitoring, all of which goes towards the estimated ten million dollars the bank lost.118

E. NORTEL

The pervasiveness of a data breach was illustrated in the hack of Nortel.119 It was recently discovered that hackers had unimpeded access to Nortel’s corporate computer system for over ten years.120 Hackers were able to steal the passwords of key executives and as such, “had access to everything.”121 As with other data breaches, the hackers were able to gain access to sensitive information such as “technical papers, research-and-development reports, business plans, employee emails and other documents.”122 The disturbing factor regarding the breach was Nortel’s

---

117 See id. (noting that Bank of America claimed it would “enhance” its data security as a result of the threat yet the scammers were still able to fraudulently access customer accounts). Wikileaks is a whistle-blowing website which has released thousands of classified documents, typically from governments or large corporations, on the internet. See Jonathan Fildes, What is Wikileaks?, BBC NEWS AND TECH. (Dec. 7, 2010), available at http://www.bbc.co.uk/news/technology-10757263.

118 See Lazarus, supra note 114 (discussing Bank of America’s response to data breach and loss of customer trust).


120 See id. (discussing hackers breach of Nortel’s computer network).

121 See id. (noting hackers had unfettered access to all of Nortel’s network).

122 Id. (detailing types of data compromised).
response -- they “‘did nothing from a security standpoint’ to try and keep the hackers out. . . .”123 Due to Nortel’s inaction, the hackers were able to remain in the company’s system and continued to monitor its activities.124

The breach and Nortel’s response likely played a major role in the company’s demise.125 As one expert put it, “[a]s far as I can tell, it’s because [Nortel] couldn’t win a contract after that because the hackers had their technical knowledge, their financials, their bids before they submitted them. How can you compete in an environment like that?”126

V. ISSUES WITH LEGAL REDRESS FOR CUSTOMERS WHOSE DATA IS STOLEN

Theft of sensitive data through sophisticated hacks, rudimentary breaches, and even low-tech means pose a significant threat to private individuals and as shown above, even large corporations and governments.127 The liability of a corporation both in the courts and the eyes of the public may depend on the sophistication of the attack and the protections in place. A company like RSA that falls prey to a sophisticated attack may be less culpable than a company like Sony,

123 Id. (noting Nortel’s failure to properly address security breach).

124 See id. (discussing report to then CEO stating that hackers still had access to Nortel’s network).


126 See id. (discussing Nortel’s loss of competiveness due to leaked proprietary and confidential information).

127 For a discussion regarding the dangers and consequences of data breaches, see supra notes 98-126.
which did not implement even the basics of data network security.\textsuperscript{128}

Customers seeking legal action against companies that inadequately protected their private data will find that the legal framework leaves little chance for success.\textsuperscript{129} This difficulty is the result of procedural hurdles and inability of proving damages caused by the threat of future identity theft.\textsuperscript{130} Additionally, current laws only require that companies promptly inform their customers of a data breach but do not create penalties if such a breach occurs, and with the exception of a few states, most laws do not outline any standard for how companies should store private customer data.\textsuperscript{131}

\begin{itemize}
  \item \textsuperscript{128} See \textit{Absolute Sownage}, supra note 26 (noting the complete lack of an intelligent security system in place at Sony).
  \item \textsuperscript{129} See \textit{Rancourt}, supra note 1 at 187-200 (discussing various difficulties faced by plaintiffs in data breach cases and low success rates of such lawsuits). See also \textit{Hammond v. Bank of N.Y. Mellon Corp.}, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *3-*9 (S.D.N.Y. June 25, 2010) (dismissing case because plaintiffs lacked standing due to claimed injuries being “hypothetical and conjectural”); \textit{Bell v. Acxiom Corp}, No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (noting plaintiff did not sufficiently prove defendant’s failure to protect client data caused injuries beyond a speculative nature); \textit{Forbes v. Wells Fargo Bank}, 420 F. Supp. 2d 1018, 1019-21 (D. Minn. 2006) (dismissing case because plaintiffs were unable to prove damages under theory of increased risk of future harm).
  \item \textsuperscript{130} For a discussion regarding the difficulties of litigating customer data breaches, see infra notes 132-170 and accompanying text.
  \item \textsuperscript{131} See \textit{Rancourt}, supra note 1, at 200-05 (discussing inadequacies of current state and federal laws which typically only require notice on part of corporation who inadequately protected customer data). For a discussion regarding federal and state laws see, infra notes 185-199.
\end{itemize}
A. COMMON LAW PROBLEMS FOR PLAINTIFFS IN DATA BREACH CLAIMS AGAINST COMPANIES

Customers who wish to pursue legal action against companies that did not properly store and protect their personal data will meet two substantial roadblocks significantly reducing their chances at receiving a favorable judgment. The two barriers that have led to almost all related cases being dismissed are standing and proof of damages.

1. STANDING: PLAINTIFFS DO NOT HAVE IT

Standing is a judicially imposed limitation on the legal process. For plaintiffs to have their case heard in court, they must have standing. To have standing, the plaintiffs must establish three elements. First, the plaintiff must have “suffered an ‘injury in fact.’” An injury in fact is where a “concrete and

---

132 See Rancourt, supra note 1 at 187 (discussing difficulties class action plaintiffs have had in seeking redress for the compromise of their personal data due to failings of defendant companies).

133 See id. at 187, 195 (noting that most plaintiffs’ claims fail as a result of lack of standing or inability to prove damages beyond a non-speculative level). See also Hammond, 2010 WL 2643307, at *1 (noting that every case court found where plaintiffs sought damages for lost personal data through data breaches have been dismissed).


135 See id. at 277 (noting courts have used standing as a means to limit individuals’ “ability to invoke the judiciary to vindicate [their] rights.”).


137 See id. (describing the first element of establishing standing).
particularized” legally protected interest is infringed.\textsuperscript{138} Additionally, such injury in fact must be “actual or imminent, not conjectural or hypothetical.”\textsuperscript{139} Second, there needs to be a “causal connection between the injury [in fact] and the conduct complained of.”\textsuperscript{140} Lastly, the injury needs to have a likelihood that it will be “redressed by a favorable decision” by the courts.\textsuperscript{141}

The norm in most state and federal courts has been to grant motions to dismiss due to lack of standing in cases regarding inadequate security of customer data.\textsuperscript{142} The vast majority of cases are dismissed because courts fail to find an injury in fact and thus

\textsuperscript{138} See id. (describing what qualifies as injury in fact). The injury in fact doctrine requires that plaintiffs demonstrate the violation of a legal interest was the cause of a “factual harm.” See Hessick, supra note 134 at 277 (discussing injury in fact rule of standing).

\textsuperscript{139} See Lujan, 504 U.S. at 560 (noting that such injury must not be conjectural but actual or imminent).

\textsuperscript{140} See id. (noting that complained injury must be “fairly . . . trace[able] to the challenged action of the defendant, and not . . . the[e] result [of] the independent action of some third party not before the court.”) (quoting Simon v. Eastern Ky. Welfare Rights Org., 426 U.S. 26, 41-42 (1976)).

\textsuperscript{141} See Lujan, 504 U.S. at 561 (noting that the likelihood of redress needs to be more than speculative).

\textsuperscript{142} See Rancourt, supra note 1 at 187-200 (noting history of courts dismissing such claims). See also Madden, supra note 12 (noting that courts have frequently held that plaintiffs lack standing because in most cases, plaintiffs can only allege increased risk of future harm).
declare that the plaintiffs lack standing. For example, the Third Circuit in *Reilly v. Ceridian Corp.* dismissed the plaintiffs’ claim of increased risk of identity theft due to a security breach based on lack of standing. In *Reilly*, the defendant corporation was responsible for managing payrolls for many clients across the country. Hackers were able to infiltrate the defendant’s database system and steal sensitive personal information. The compromised information consisted of social security numbers, birthdates, addresses, and bank account numbers associated with direct deposit. The plaintiffs brought suit alleging that the defendant’s inadequate security caused them to suffer an increased risk of future identity theft, emotional distress, as well as the costs of needing to monitor their credit. In affirming the district court’s dismissal, the Third Circuit held that

---

143 See e.g., *Reilly v. Ceridian Corp.*, 664 F.3d 28, 40 (3d Cir. 2011) (upholding lower court’s determination that increased risk of identity theft did not create standing for plaintiffs); *Amburgy v. Express Scripts Inc.*, 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009) (holding that risk of future identity theft was not sufficient to establish standing); *Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705, 712-13 (S.D. Ohio 2007) (ruling in favor of defendant’s summary judgment motion because plaintiff was not able to establish actual injuries from loss of personal information); *Hendricks v. DSW Shoe Warehouse*, 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006) (dismissing plaintiffs’ claim, finding that need for credit monitoring does not constitute actual injury).

144 664 F.3d 28 (3d. Cir. 2011).

145 See *Reilly*, 664 F.3d at 40 (affirming lower court’s ruling that plaintiffs lack standing).

146 See *id.* (discussing defendant’s line of work and how it related to plaintiffs).

147 See *id.* (noting that hackers gained access to sensitive information of approximately “27,000 employees at 1,900 companies”).

148 See *id.* (detailing information potentially accessed by hackers but also noting that it was unclear whether or not “hackers read, copied, or understood the data”).

149 See *id.* (outlining plaintiffs allegations).
there needed to be more than just a speculative or hypothetical possibility of injury, and instead there needs to be a concrete or imminent injury suffered.\footnote{See id. at 41-43 (discussing holding in \textit{Lujan} and \textit{Whitmore} and reiterating that the mere possibility of future harm is not enough to meet the standing standards).} Furthermore, the court emphasized that because there was no proof that the hackers even stole or understood the data, the imminent nature of the alleged harm was greatly reduced.\footnote{See id. at 43-44 (distinguishing the present case from \textit{Pisciotta v. Old Nat. Bancorp}). \textit{In Pisciotta}, the Seventh Circuit found that standing was established based on the increased risk of future identity theft resulting from a data breach. \textit{See Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 638-39 (7th Cir. 2007) (holding that standing standard was met by relating data breach related harms to toxic tort where injury has resulted but not yet manifested)}. For a further discussion of \textit{Pisciotta see infra} notes 164-168 and accompanying text.} Accordingly, the Third Circuit affirmed the dismissal, leaving the plaintiffs without a cause of action unless an actual identity theft occurs\footnote{See \textit{Reilly}, 617 F.3d at 40 (dismissing plaintiffs’ case). It is important to note that the court here distinguished the present case from toxic torts because in toxic torts, the damage had already occurred but manifestation is unexpected, whereas in the present case, no actually damage nor change in status quo occurred. \textit{See id. at 45}.}.

A similar result was reached by the Eastern District of Missouri in \textit{Amburgy v. Express Scripts Inc.},\footnote{671 F. Supp.2d 1046 (E.D. Mo. 2009).} where the court granted the defendant’s motion to dismiss and held that the plaintiffs’ risk of future identity theft was not enough to establish standing.\footnote{See \textit{Amburgy}, 671 F. Supp. 2d at 1053 (holding that plaintiffs’ claim of future threat of identity theft was not enough to establish standing). \textit{See also} \textit{Rancourt, supra} note 71 at 190-91 (discussing court’s dismissal of claim for lack of standing even where injuries were “more particularized”).} There, the plaintiffs alleged that the defendant’s inadequate security of its database system allowed
“unauthorized persons to gain access to confidential information.” 155 The compromised information included social security numbers, birthdates, and prescription information. 156 As a result of the data breach, the plaintiffs claimed that they suffered an “increased risk of becoming victims of identity theft.” 157 Additionally, the plaintiffs claimed that they lost the exclusive use of their prescription information and were forced to continually monitor their accounts in order to prevent potential financial harm. 158 In dismissing the case, the district court stated that an alleged injury must be “actual or imminent, not conjectural or hypothetical.” 159 The court importantly noted that there were too many “ifs” that needed to come to pass in order for the plaintiffs to suffer the alleged harm or injury. 160

Despite the difficulties discussed above, a splintering has begun to occur among the different

155 See Amburgy, 671 F. Supp. 2d at 1049 (discussing plaintiff’s claims against defendant).
156 See id. (noting type of information which was compromised as a result of the breach of the defendant’s network).
157 See id. (detailing plaintiffs’ allegations against defendant).
158 See id. (noting plaintiffs’ claims of damages and injuries as a result of defendant’s inadequate security of its network). See also Rancourt, supra note 1 at 190-91 (outlining Amburgy suit).
159 See Amburgy, 671 F. Supp.2d at 1052 (stating that “[t]he Supreme Court has ‘emphasized repeatedly’ that the alleged injury ‘must be concrete in both a qualitative and temporal sense. The complainant must allege an injury to himself that is distinct and palpable, as opposed to merely abstract, and the alleged harm must be actual or imminent, not conjectural or hypothetical.’”) (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)). The court additionally noted that though “imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative. . . .” See id. at 1052 (internal quotation omitted).
160 See Amburgy, 671 F. Supp. 2d at 1053 (detailing how plaintiffs’ claims were too hypothetical).
district courts regarding standing. While the majority of courts keep true to the injury in fact test of *Lujan*, which requires an actual or imminent harm, some courts have expanded the rule by holding that victims of data breaches can establish standing through potential future harm. For example, the court in *Pisciotta v. Old Nat. Bancorp* found that the risk of future harm did confer standing. In *Pisciotta*, the plaintiffs brought a class action suit against the defendant alleging that because of the defendant’s lack of adequate security measures, hackers were able to gain access to the plaintiffs’ sensitive personal information. The plaintiffs argued that they were harmed by the increased risk of future identity theft and that they needed to be compensated for credit monitoring services which were needed to protect against potential future identity theft. Breaking from the majority of cases, the Seventh Circuit held that the plaintiffs had standing, stating without much discussion, that the “injury-in-fact requirement can be satisfied by a

---

161 *See Hammond*, 2010 WL 2643307, at *1-*2 (noting a split between courts on how to analyze data breach claims against companies).
162 *See e.g., Pisciotta*, 499 F.3d at 632 (holding plaintiffs have standing because of risk of future harm due to data breach); Krotter v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010) (finding plaintiffs have standing in data breach claim). *But see Reilly*, 664 F.3d at 40 (refusing to follow *Pisciotta* and holding that plaintiffs lacked standing to bring suit); *Amburgy*, 671 F. Supp. 2d at 1053 (holding that risk of future identity theft was not sufficient to establish standing).
163 499 F.3d 629 (7th Cir. 2007).
164 *See id.* at 631 (holding plaintiffs had standing but dismissing case for lack of compensable damages). The court nevertheless dismissed the case because the plaintiffs were unable to prove damages. *See id.*
165 *See id.* at 631-33 (discussing plaintiffs’ allegations against defendant).
166 *See id.* at 631-32 (discussing plaintiffs’ claims and what they sought as damages).
threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant’s actions.”\textsuperscript{167} Although the court ruled that the plaintiffs had standing, the case was nevertheless dismissed because the court found that the need for credit monitoring did not give rise to compensable damages.\textsuperscript{168}

The current state of the law makes it so most cases are unable to make it past the standing barrier.\textsuperscript{169} Any cases that overcome the standing hurdle are still likely to be dismissed for failure to prove damages.\textsuperscript{170}

2. PROVING DAMAGES FOR POTENTIAL HARM

Some plaintiffs have been able to meet the standing burden if they bring their case in a favorable jurisdiction, but these plaintiffs encounter another roadblock to the successful outcome of their case; proof of damages.\textsuperscript{171} Often, the majority of class action plaintiffs will typically not have suffered any actual harm as a result of the data breach but rather a possibility

\textsuperscript{167} See id. at 634 (holding that plaintiffs had standing to bring claim).

\textsuperscript{168} See id. at 637-40 (dismissing claim for failure to prove compensable damages).

\textsuperscript{169} For a discussion regarding standing in data breach claims, see supra notes 134-170 and accompanying text.

\textsuperscript{170} See Hammond, 2010 WL 2643307, at *1 (noting that though some courts will find standing in data breach cases, they are nevertheless dismissed for failure to prove actual damages).

\textsuperscript{171} See Madden, supra note 11 (noting that where cases have been able to make it pass the standing hurdle, claims are typically dismissed for failure to state claim because “potential future harm [is] too speculative to support a claim for damages”). See also Pisciotta, 499 F.3d at 632 (dismissing plaintiffs’ claims, holding that plaintiffs did have not direct losses or damages as a result of the data breach);
of future identity theft. To survive dismissal, there must be damages that are capable of being redressed. In data breach claims, where plaintiffs are suing the companies for inadequately protecting their personal data, there is usually little proof of exactly what was stolen and in what form. Furthermore, with the exception of those who have actually had their identities stolen, plaintiffs are suing for hypothetical and potential damages.

In Pisciotta, the plaintiffs were able to meet the standing burden, but the court still affirmed the dismissal on the grounds that paying for credit monitoring services was not something that could be compensated. In making its determination, the court looked to the law enacted by the Indiana legislature which requires that companies promptly notify their customers if a data breach occurs, but does not create a private right of action or a duty for the company to compensate its

---

172 See Hammond, 2010 WL 2643307, at *1 (discussing typical data breach claims and their lack of actual damages). See also Rancourt, supra note 1 at 195 (noting that in most cases, data breach victims lack “definitive proof that [the stolen] information has actually been misused”).

173 See Shafran v. Harley-Davidson Inc., No. 07 CIV. 01365 (GBD), 2008 WL 763177, at *2 (S.D.N.Y. Mar. 20, 2008) (noting that without more, the “time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy.”).

174 See Rancourt, supra note 1 at 195 (discussing plaintiffs inability to prove the misuse of stolen data in typical data breach cases).

175 See id. at 195-97 (noting that damages need to be actual rather than speculative for plaintiffs to be able to state a claim which will not be dismissed).

176 See Pisciotta, 499 F.3d at 638 (affirming lower court’s dismissal of the case).
Accordingly, the court held that although standing was conferred due to the increased chance of future identity theft, dismissal was still appropriate because of the lack of compensable injuries.\(^{178}\)

Dismissal due to lack of compensable injuries can be further seen in \textit{McLoughlin v. People’s United Bank Inc.}\(^{179}\) In \textit{McLoughlin}, the plaintiffs brought suit against the defendant for negligence due to lost personal and banking data that arose out of a data breach at The Bank of New York Mellon.\(^{180}\) The data breach occurred through a low-tech method; the back-up files were stolen off of a truck.\(^{181}\) The Connecticut District Court was persuaded by the reasoning in \textit{Pisciotta} and found that the plaintiffs had standing.\(^{182}\) Consistent with the problem in most data breach cases, the plaintiffs had not yet suffered identity theft but were claiming an increased

\(^{177}\) See id. at 637-38 (finding that Indiana legislature did not likely intend the costs of credit monitoring to be a form of compensable damages stating “[h]ad the Indiana legislature intended that a cause of action should be available against a database owner for failing to protect adequately personal information, we believe that it would have made some more definite statement of that intent.”).

\(^{178}\) See id. (affirming dismissal of case because lack of compensable damages).


\(^{180}\) See id. at *1 (discussing plaintiffs’ claim against defendant).

\(^{181}\) See id. (discussing how data breach occurred). It is important to note that though The Bank of New York Mellon encrypted the social security numbers of the defendant’s customers on its online database, the backup files were not encrypted. See id. Additionally, it can be assumed to be more difficult to orchestra a robbery of physical backups from a company owned truck as opposed to the simple SQL injection hacks that brought down Sony which can be done easily at one’s own home. For a discussion of the Sony hacks and methods used, see supra notes 25-76 and accompanying text.

\(^{182}\) See McLoughlin, 2009 WL 2843269, at *3-*4 (discussing general move by courts to find standing in data breach cases and accordingly finding that plaintiffs had standing).
risk of potential identity theft.\textsuperscript{183} In dismissing the case, the court stated that “the courts of Connecticut, like those of New York, would not recognize a negligence claim founded solely on the fear, unsupported by any allegation of malfeasance, of identity theft. . . .”\textsuperscript{184}

B. FEDERAL AND STATE LAW INADEQUACIES

Customers who are unable to bring successful claims under case law will also find the federal and state laws inadequate to address the failure of companies to properly protect their stored private data.\textsuperscript{185} The current statutory framework in the United States requires companies to merely inform their customers when their data has been compromised promptly; the majority of laws do not require more of the companies, nor do the

\begin{flushright}
\textsuperscript{183} See id. at *6-*9 (discussing plaintiffs’ allegations against defendant and noting pure speculative nature of claims). Additionally, the plaintiffs never alleged what happened to the backup files and it was also unclear whether they were lost or stolen. See id. at *1, *7.
\end{flushright}

\begin{flushright}
\textsuperscript{184} Id. at *8 (holding that without actual damages, a claim of negligent protection of data could not stand). The court noted that:
\end{flushright}

actual damages are a necessary element of any claim sounding in negligence. While no Connecticut Court has ever held that an increased risk of identity theft is insufficient to establish actual damages, the Plaintiffs have pointed to no case decided anywhere in the country where a court allowed a negligence claim to survive absent an allegation of actual identity theft. See id.

\begin{flushright}
\textsuperscript{185} See Rancourt, supra note 1 at 200-02 (detailing why individuals bring common law claims against companies for breach of contract and negligence due to the lack of adequate statutory options). See also Madden, supra note 11 at 27-28 (discussing inability of plaintiffs in data breach cases to successfully bring claims in court).
\end{flushright}
laws currently address forms of punishment for failure to protect such data.\textsuperscript{186}

On the state level, the majority of laws require only that companies promptly notify their customers...

\textsuperscript{186} See Rancourt, \textit{supra} note 1 at 200-202 (noting current federal and state laws focus on hackers not on individuals and also only impose penalties on companies for failure to report, not for inadequate security of their database networks). \textit{See generally} Stored Wire And Electronic Communications and Transaction Records Access 18 U.S.C. §§ 2701-12 (2006) (punishing unauthorized access of stored electronic communications and outlining mandatory and voluntary disclosure of stored communications but silent on storage guidelines or standards); Computer Fraud & Abuse Act, 18 U.S.C. § 1030 (2000 & Supp. 2011) (punishing unauthorized computer access but not defining security guidelines); 15. U.S.C. §§ 6801-09 (requiring financial institutions to disclose when information is compromised). \textit{See also generally} CAL. CIV. CODE §§ 1798.80-84 (West 2009) (requiring disclosure for data breach and merely reasonable security measures without defining such measures); DEL. CODE ANN. TIT. 6, §§ 12B-101-04 (2005) (requiring disclosure in case of data breach and giving only Delaware Attorney General authority to enforce); FLA. STAT § 817.5681 (2005) (requiring disclosure when there is a data breach); N.J. STAT. ANN. 56:8-163 (West Supp. 2011) (requiring and defining disclosure and notice procedures if data breach occurs); S.C. CODE ANN. § 39-1-90 (2010) (requiring notice in case of unauthorized access to online databases); VA. CODE ANN. § 18.2-186.6 (West 2008) (requiring notice when data breaches occur). \textit{But see} 201 MASS. CODE REGS. §§ 17.00-17.05 (2008) (requiring “e]very person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards.”); NEV. REV. STAT. § 603A.010 \textit{et seq.} (2010) (requiring encryption of stored data along with disclosure).
when a data breach occurs. Some states have gone further to require that companies encrypt their customer data. The shortcoming of state laws is that the majority do not require any minimum level of security standards, and often do not give customers a private right of action should a company fail to install adequate security measures. Additionally, because most state laws only require prompt notification, once a company notifies its customers of a data breach they no longer are statutorily liable even if they had non-existent security measures. More troubling is that some state laws

187 See e.g., CAL CIV. CODE §§ 1798.80-84 (West 2009) (requiring disclosure for data breach and merely reasonable security measures without defining such measures); DEL. CODE ANN. TIT. 6 §§ 12B-101-04 (2005) (requiring disclosure in case of data breach and giving only Delaware Attorney General authority to enforce); FLA. STAT § 817.5681 (2005) (requiring disclosure when there is a data breach); N.J. Stat. Ann. 56:8-163 (West Supp. 2011) (requiring and defining disclosure and notice procedures if data breach occurs); S.C. CODE ANN. § 39-1-90 (2010) (requiring notice in case of unauthorized access to online databases); VA. CODE ANN. § 18.2-186.6 (West 2008) (requiring notice when data breaches occur).

188 See 201 MASS. CODE REGS. §§ 17.00-17.05 (requiring “[c]very person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards.”); NEV. REV. STAT. ANN. § 603A.010 et seq. (requiring encryption of stored data along with disclosure).

189 See supra note 186 (noting need to disclose but lack of guidance on security standards).

190 See supra note 186 (creating liability only when companies or entities fail to promptly notify customers of data breach and in some cases only allowing enforcement by Attorney General). See also Jill Joerling, Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data, 32 WASH. U. J.L. & POL’Y 467,471-85 (2010) (detailing how many state laws do not allow for private action but rather put enforcement in hands of Attorney Generals as well as exempting companies from notification if information stolen in breach was encrypted).
exempt companies from the need to notify their customers of a data breach if the company used encryption technology to store the data.\textsuperscript{191}

Most federal statutes mirror their state counterparts, only requiring that companies disclose to their customers when a data breach occurs.\textsuperscript{192} These laws do not detail how companies should store the data nor delineate any minimum standards for companies to follow.\textsuperscript{193} The laws create causes of action against the hackers who breached the networks but they remain silent with regard to companies such as Sony who recklessly and negligently store sensitive customer data.\textsuperscript{194} Because state laws are nonconforming in their approaches, federal laws may be better suited to address future standards and issues for data security.\textsuperscript{195}

\textsuperscript{191} See Joelring, supra note 190 (discussing companies exemption from some state disclosure requirements if data stolen was encrypted).

\textsuperscript{192} See supra note 186 (noting lack of minimal standards for companies in statutes and laws only requiring prompt notice after breach is detected). See also Rancourt, supra note 1 at 200-204 (discussing inadequacies of federal law).

\textsuperscript{193} See Rancourt, supra note 1 at 200-203 (discussing lack of minimum standards for security in the law but rather focus on punishing those who did hack only).

\textsuperscript{194} See Rancourt, supra note 1 at 201-202 (exemplifying federal law and the creation of criminal liability for hacking databases but lack of standards or guidelines to secure data).

Currently, plaintiffs see little help from state laws in trying to redress their damages as a result of the inadequate security in place by companies, but the tides may be changing.\textsuperscript{196} The prevalence of e-commerce, the publicity of high profile data breaches, and privacy concerns has fostered more public awareness as well as legislative acknowledgement of the need for database security.\textsuperscript{197} This increase in awareness has led to newer state laws, such as Nevada’s, which requires companies that store data encrypt sensitive customer information.\textsuperscript{198} Companies should get ahead of this changing legal environment and take the appropriate steps to protect their customer data, not only to prevent future legal liability, but also to maintain customer trust, market share, and profitability.\textsuperscript{199}

VI. FUTURE POLICY CONSIDERATIONS FOR COMPANIES

Companies have much to lose if they continue, as Sony did, with minimal or non-existent security measures.\textsuperscript{200} Not only do companies face the threat of litigation and the costs that come with a legal defense, they also face loss of market share, customer mistrust, lowered share prices, lost revenue, and even implicit economic costs, such as wasted resources and lost opportunity costs.\textsuperscript{201} It is important for companies to

\textsuperscript{196} For a discussion regarding statutory inadequacies, see supra notes 185-199 and accompanying text.
\textsuperscript{197} See Greenwald, supra note 195 (noting growing interest in need for federal legislation regarding data breaches).
\textsuperscript{198} See NEV. REV. STAT. ANN. § 603A.010 \textit{et seq.} (requiring encryption of stored data along with disclosure).
\textsuperscript{199} For a discussion regarding the benefits of implementing appropriate security measures, see infra notes 200-232 and accompanying text.
\textsuperscript{200} For a discussion regarding the impacts of data breaches on companies, see supra notes 92-126 and accompanying text.
\textsuperscript{201} For a discussion regarding the explicit and implicit costs of not implementing adequate security policies and procedures, see infra notes 203-217 and accompanying text.
consider these issues before they decide to write off network security as an unimportant expense. The prudent company should instate an effective security policy that will sufficiently protect their customer’s data.  

A. LEGAL CONSIDERATIONS

Currently, companies creating policies for storing customer data have little to fear by way of litigation for failure to properly protect customer data. As discussed above, plaintiffs bringing claims against companies for security breaches face an uphill battle. Although companies can currently create policies without much fear of legal ramifications, the state of the common law and statutory law are likely to change to reflect the new prevalence of e-commerce and companies should act accordingly. This shift can be seen by the courts that have found standing for potential future identity theft. The changing legal environment is further exemplified by Countrywide’s recent settlement for the theft and attempted sale of personal information

---

202 For a discussion regarding policy and procedure suggestions for database security, see infra notes 218-232 and accompanying text.
203 For a discussion regarding the inability for plaintiffs to successful seek legal redress against companies in data breach cases, see supra notes 132-184 and accompanying text.
204 For a discussion regarding the standing and proof of damages burdens plaintiffs face, see supra notes 132-184 and accompanying text.
205 For a discussion regarding the current common law and statutory environment of data breach claims and the slow move towards new legislation, see supra notes 132-199 and accompanying text.
by a senior financial advisor. The Countrywide claim involved an insider at Countrywide who stole millions of customers’ information and sold it to third parties. Countrywide agreed to provide two years of free credit monitoring, identity theft insurance, and to pay approximately $3.5 million in attorney’s fees. With the potential loss of the legal monopoly companies have on plaintiffs, it would be prudent and cost effective for companies to install more stringent security measures for their stored customer data in order to fend off potential litigation.

B. FINANCIAL AND OTHER COMPANY CONSIDERATIONS

There are financial concerns which should be taken into account when creating security policies which go beyond protecting customer data. As seen in the Nortel case above, companies should have strong incentives to protect the data on their networks. If

---


207 See id. (discussing claims).


209 For a discussion of legal state of data breach claims, see supra notes 132-184 and accompanying text.

210 See Rashid, supra note 17 (noting that average total cost for company for one data breach is approximately 7.2 million dollars).

211 For a discussion regarding the Nortel data breach and its financial impacts, see supra notes 119-126 and accompanying text.
hackers can gain access to customer data, it is likely that they also have access to sensitive company data.\textsuperscript{212} Such a breach can take away a company’s competitive advantage, give away proprietary information, give hackers insight into the financial health of the company, as well as drive customers to competitors.\textsuperscript{213}

Additionally, data breaches can result in massive losses, as Bank of America saw when the company lost over ten million dollars as a result of a security breach.\textsuperscript{214} These losses are particularly disturbing to shareholders because they represent not just lost assets, but also lost opportunities to further shareholder and company interests.\textsuperscript{215} Moreover, as Sony exemplifies public exposure of inadequate network security and massive losses of sensitive customer data can result in significant drops in the stock price of publicly traded companies.\textsuperscript{216}

\textsuperscript{212} For a discussion regarding the downfall of Nortel and how the data breach played a major role in the failure of the company, see supra \textsuperscript{119-126} and accompanying text.

\textsuperscript{213} For a discussion regarding data breaches, the types of information that are typically stolen and potential loss of market share, see supra \textsuperscript{notes 92-126} and accompanying text.

\textsuperscript{214} For a discussion regarding Nortel’s loss of its competitive advantage and eventual bankruptcy, see supra \textsuperscript{notes 119-126} and accompanying text.

\textsuperscript{215} For a discussion regarding the financial costs of the data breach of Bank of America as well as the massive financial losses of Sony due to their massive data breach, see supra \textsuperscript{notes 25-91, 113-118} and accompanying text. Additionally, if companies put adequate security measures in place in the first place, they would likely reduce the money spent to remedy such breaches and thus have more money to invest in other areas of the business. It is estimated that approximately forty-one percent of data breaches occur simply due to company negligence. \textit{See} Rashid, supra \textsuperscript{note 17} (noting that negligence is the most common cause of data breaches).

Further, such breaches can endanger the long-term viability of a company by reducing market share, causing a loss of customer trust, and ultimately a loss of a company’s customer base.\textsuperscript{217}

C. SUGGESTIONS FOR FUTURE POLICIES AND PROCEDURES

Companies should focus on two major areas when creating a security policy to protect stored customer data. First, companies should implement adequate security procedures, such as encryption technologies, to ensure that if a data breach does occur, the data stolen will still be protected.\textsuperscript{218} Second, should a data breach occur, companies should immediately notify their customers to allow them the opportunity to protect their identities from possible theft.\textsuperscript{219}

1. SECURITY PROCEDURES

Companies’ first concern should be to take adequate steps to prevent a data breach from occurring in the first place.\textsuperscript{220} Sony had almost no security measures in place to protect their customer data, and their networks were ripped apart in a matter of two months by

\textsuperscript{217} See Rashid, supra note 18 (noting customers leaving companies, resulting in a four percent turnover rate, an average 4.5 million dollars loss of business through lost sales and employees being diverted to data breach resolution). For a discussion of the market effects of data breaches, see supra notes 200-217 and accompanying text.

\textsuperscript{218} For a discussion regarding the need for adequate security procedures, see supra 77-91 and accompanying text.

\textsuperscript{219} For a discussion of the need to quickly notify customers of a breach, see supra notes 77-91 and accompanying text.

simple SQL injection attacks.\textsuperscript{221} Such an easy breach should not have occurred, especially not against such a wealthy and respected company.\textsuperscript{222} Accordingly, companies should take the appropriate steps to prevent unauthorized access.\textsuperscript{223} There should be institutional controls designed to prevent unauthorized use of customer files by employees of the company, database security measures in place to prevent known methods of database attacks, and encryption technology should be used on information which is not publicly available.\textsuperscript{224} Additionally, companies should have monitoring procedures in place facilitating quick detection of attempted or successful breaches which would allow the company to take the appropriate steps in response to a breach.\textsuperscript{225} A company that implements such controls and policies will be better protected from legal liability and will likely not go through the public shaming that Sony experienced if a breach occurs. Indeed, such steps will not only make it more difficult for hackers to access customer data, but they will help reduce potential legal fees, loss of market share, and other financial woes which companies in the past have experienced as a result of negligent database security.\textsuperscript{226}

2. AFTER THE BREACH

Not all data breaches are preventable. As was shown in the RSA case, even the most sophisticated

\textsuperscript{221} For a discussion of the Sony data breaches, see supra notes 25-91 and accompanying text.
\textsuperscript{222} See id.
\textsuperscript{223} For a discussion regarding ramifications and examples of such, see supra notes 92-126 and accompanying text.
\textsuperscript{224} See Baccam, supra note 220 at 2-13 (discussing methods to effectuate proper security plan).
\textsuperscript{225} See id. at 10-11 (discussing need and benefits of auditing security systems).
\textsuperscript{226} For a discussion of the financial ramifications of data breaches, see supra notes 200-217 and accompanying text.
Accordingly, companies should have procedures in place to immediately notify customers if a breach does occur. As the Sony case illustrated, notification a week after a breach is unacceptable as a week in the context of data breaches is a lifetime. Customers need immediate notification so they can quickly take the appropriate measures to protect their identities and financial wellbeing, as well as have a heightened alertness for possible scammers. Such policies will help mitigate the loss of trust which can occur after a customer’s data is compromised, and will help to mitigate the outflow of customers to competitor companies. Importantly, failure to quickly notify is currently the one avenue that may expose a company to legal liability, as many state and federal statutes require prompt notification if a breach occurs.

VII. THE TAKEAWAY

When examining the hacker attacks on all aspects of Sony’s business, the ramifications for failing to provide sufficient security measures to protect stored

\[\text{\textsuperscript{227}}\text{For a discussion regarding the highly sophisticated hacker attack on RSA, see supra notes 98-106 and accompanying text.}\]
\[\text{\textsuperscript{228}}\text{For a discussion regarding the statutory requirements to notify customers of a data breach, see supra notes 185-199 and accompanying text.}\]
\[\text{\textsuperscript{229}}\text{For a discussion regarding Sony’s response to the data breaches and its inadequacies, see supra notes 77-91 and accompanying text.}\]
\[\text{\textsuperscript{230}}\text{For a discussion regarding the importance of prompt notification after a data breach, see supra notes 82-86 and accompanying text.}\]
\[\text{\textsuperscript{231}}\text{For a discussion regarding the loss of trust among customers after a data breach, see supra notes 200-217 and accompanying text.}\]
\[\text{\textsuperscript{232}}\text{For a discussion regarding the statutory need to notify customers if a breach occurs, see Supra notes 185-199 and accompanying text.}\]
customer data become clear.\textsuperscript{233} It is important to note that although the current legal framework allows companies to be shielded from legal liability for their negligence, they may still incur substantial costs through financial and market share losses.\textsuperscript{234} It is also important to note that with the higher prevalence of e-commerce, privacy issues, and the wide publicity of big name company data breaches, the procedural protections companies have may soon be worn away.\textsuperscript{235} In the face of the potential consequences when compared to the expenses of implementing appropriate security measures, it becomes clear that companies and customers have a shared interest in the proper protection of sensitive customer data and that companies should take the steps to implement sufficient security measures.

\textsuperscript{233} For a discussion regarding the data breaches at Sony and the effects it had on Sony’s business, see \textit{supra} notes 25-91 and accompanying text.

\textsuperscript{234} For a discussion regarding the legal landscape in data breach claims against companies for negligence and other common law theories, see \textit{supra} notes 132-184 and accompanying text.

\textsuperscript{235} For a discussion regarding the changing of state and federal laws, see \textit{supra} notes 185-199 and accompanying text.
I. INTRODUCTION

This paper represents a think piece exploring early considerations of a new way of understanding and countering decision-making influence affected by Cyber Warfare payloads (where ‘cyber’ implies the use of any technology between sender/recipient). The approach detailed uses a form of Analogical Research (AR) to extract value from a biological model, in this case the effects that parasites exercise on their hosts. There is a lot to learn from parasites and the response of infected organisms - and the analogy has (as it were) legs.

The author’s argument is that just as parasites manipulate their hosts’ behavior, if we think of the informational payload (memes) of cyber-warfare as parasites, then we could perhaps more effectively understand, counter or develop such artifacts.

The author originally stumbled upon the potential relevance from understanding the actions of parasites as a way of conceptualizing problematic human
behavior: in particular, the phenomenon of suicide terrorism. Rather than falling back on various explanations rooted in conventional wisdom, pop psychology or oppression, the author suggests instead that behavior change could be thought of as the result of being ‘infected’ by the equivalent of a parasitic set of memes which transform the behavior and rationale of an individual thereby enabling them to choose to be a suicide bomber.

Parasites achieve their effects and conceal their existence through a myriad of subtle and sophisticated operations (endocrinal, neurochemical). If, for example, a parasite can transform the risk-taking behavior, preferential food choice and emotional reward of complex organisms, perhaps parasitic assemblages of memes could be changing the risk profile, preferential information sources and emotional rewards that suicide bombers (and their supporters) access and gain respectively.

Having consulted extensively in Information Warfare / Operations, cyber-security and the protection of commercial and strategic decision-makers the author is aware of the openness of defense and security practitioners and policy-makers to new ideas. Given a certain familiarity and a deep empathy with the challenges that face these communities, the author hopes that other share his enthusiasm for exploring the potency of any approach to the developing theatre of cyberspace. The author draws on his professional training in social anthropology to develop a new way of making (potential) sense of an established problem. The conclusion of this paper is to suggest that the parasitological analogy is an important and powerful one that offers the prospect of both better understanding threats and developing counter-measures. Not least, asymmetric thinking provides liberal democratic states
with competitive advantage by absorbing and exploiting innovative perspectives.

II. THE POWER OF ANALOGICAL RESEARCH (AR)

No matter how strong the urge or imperative, it’s generally very difficult to credibly set out to ‘think outside the box’. There has to be some catalyst or trigger from which new thoughts can spring. Author’s ‘writer’s block’; the artist’s blank canvas; the sculptor’s uncarved block; the strategic leader with their on-tap ‘blue sky thinker’ ... all need initiation to begin work from some external source. This author finds biological analogies a powerful source of innovative thinking. Some years ago, in working closely with deeply technical experts in the domain of computer security, I floated the idea of drawing on the area of biology charged with understanding predator-prey interaction.

The lay-person might imagine that ecosystems change little and slowly and that battles between predator and prey alter little. However, this is proven not to be true. In Australia, the introduced Cane Toad (a failed form of biological control for a pest of the sugar cane – a failure because of the ability of the target pest beetle to climb sugar cane, a feat that toads have yet to master) proved a toxic invader of the native ecosystem. A voracious appetite, fast reproductive rate and highly toxic poison concealed within its skin made the toad a highly effective new entrant into Australian habitats.

On closer inspection, however, Australian indigenous wildlife responded incredibly rapidly to the arrival of the invader toad. Domestic species have quickly learned, for example, how to consume the edible parts of these large amphibians by not eating the parotid glands.

So, the learning point is that an ecosystem model of computer network security would ideally be made capable of learning about a completely new form of
security vulnerability - and dispatches it swiftly. If the lesson works in nature there is no reason why the principles cannot (by analogy) be translated into and implemented for an alternative type of ecosystem.

III. THE PROBLEM: UNDERSTANDING HOW CYBER WARFARE PAYLOADS MAY CHANGE HUMAN BEHAVIOR

Although we all like to consider ourselves as highly rational and sensible beings, the fact remains that if we expose ourselves to objective analysis (via some kind of reflection on practice; discussions with a therapist or counselor; re-examination of decisions), we will no doubt find that we are a lot less rational than we had hoped. Perceptions, beliefs, prejudices, assumptions, models, these and other artifacts guide, shape and constrain our decisions. How this operates as a cohesive whole is a tricky issue for interdisciplinary attention.

However, changing human behavior is something that we can focus on, specifically if it relates to problematic behavior. So, antisocial behavior in public places; unwanted employee activity; misfits … these are all difficult phenomena that we would like to understand better and for which no easy answers exist.

If a cyber-warfare payload (however delivered) achieves its effect – it changes human behavior either in a specifically desired way (e.g. a change of opinion on a political cause) or perhaps simply makes an existing process unreliable (e.g. introducing unexpected information into a decision-making process).

What one is very short of in general terms are neat conceptualizations of how information changes behavior. As progress in neuroscience develops, it is increasingly possible to map (in real time) how the brain responds to information – it’s going to be problematic to understand why the brain accepts or seeks out specific information and actively undergoes pretty significant
changes (cf. from a teaching assistant to a committed suicide bomber). Note that in relation to the 7/7 bombers in the UK there is little in their backgrounds which mark them out as particularly vulnerable to radicalization [...] they were] apparently well integrated into British society’.

“[T]he vast majority of suicide bombers, the 7/7 four included, show no sign of mental illness and have no criminal history. They are often better educated than their peers and hold respectable jobs. The backgrounds of the 4 men appear largely unexceptional[...]. We do not know how Khan developed his extreme views or precisely when.”

The power of the analogy on which I draw in this paper is not to explain per se exactly how the brain is influenced by information, rather to suggest that the analogy might provide us with enhanced understanding of how the brain may be thought of as being influenced. In itself, this may provide alternative understandings and insights for both offensive and defensive purposes.

By necessity, it is now vital for me to speedily explain some of the mechanisms by which parasites secure behavior change in their hosts.

---

IV. CASE STUDIES OF SIGNIFICANT BEHAVIOR CHANGE ACHIEVED THROUGH NEUROTRANSMITTER MODIFICATION BY PARASITES

Although many parasites cause minimal changes in their host’s behavior or health, some produce substantial alterations which are directly linked to the requirements of the parasite to continue their lifecycle (moving into another host for example). A good example is that of rats who are infected with *Toxoplasma gondii*. Here, the rodents “show an increase in their exploratory behavior, thereby increasing, at least indirectly, the likelihood of predation by feline definitive hosts”.

A different parasite - *Eimeria vermiformis* – produces a mirror image of this behavior change: where rats lose their normal wariness and risk-aversity when they encounter a potential predator. Instead, “this behavior becomes subdued, suggesting the possibility that the parasite is increasing the likelihood of the host’s predation”.

What is most interesting, apart from the somewhat gruesome dimensions of such examples, is the means by which seemingly innate behaviors are overcome. Naturally, this has to be a complex mechanism to achieve such an outcome: “It appears that the abnormal behavior of the host is due, in part, to parasite-induced changes in the serotonin neuromodulatory system, and to an opioid-mediated...

---


analgesia”. 6 Another way of describing this is as where
the parasites “actively target the host’s neuroendocrine
systems”. 7

In other words, the fundamental behaviors and
reactions of the host are overcome and re-programmed
by the parasite. To transform a wary and cautious animal
into a hasty and reckless one is quite an achievement.
Add to that an increased ability to withstand pain by
sensing it less without, I assume, fleeing - and the
parasite has ensured that its host is as optimally likely to
assist in achieving its next life stage (by sacrificing itself
to a predator with retarded escape responses) as possible.

To unpack the complex mechanism – excretions
from parasites interfere with normal neurotransmission.
In the case of *Eimeria vermiformis*, it is the serotonin
pathways in the brain which are modified. In the human
brain, serotonin is responsible for regulating mood,
appetite, sleep as well as being involved in processes of
memory and learning. In the animal model, it influences
how the gut works and how the animal perceives the
availability of food. It also appears that many other
activities can be enhanced or depressed as a response to
the perception of food availability.

Serotonin is relevant in the case of the effects of
the parasitic worm because it shapes the ‘fight or flight’
response of the rat. In other animals it modulates the
response by enhancing it in socially dominant pack
animals and inhibiting it in subordinates. The swarming

6 Albert O. Bush, Jacqueline C. Fernandez, Gerald W. Esch and
J. Richard Seed, *Parasitism; The Diversity and Ecology of Animal

7 Jenny Carolyn Shaw, Wayne J. Korzan, Russ E. Carpenter,
Armand M. Kuris, Kevin D. Lafferty, Cliff H. Summers, CH and
Øyvind Øverli, *Parasite manipulation of brain monoamines in
California killifish (Fundulus parvipinnis) by the trematode
Euhaplorchis californiensis*, 276 PROC. R. SOC. B, 1137, 1137-
1146 (2009).
of normally non-social locusts is also triggered by serotonin – but only when food supply is perceived to have declined. In addition to the increased ‘gregariousness’ of these locusts, they undergo physical transformation: a darkening in color changes and increase in muscle size. Indeed, swarming and non-swarming locusts look so different that they were originally thought to be separate species.8

California Killifish – infected by another form of parasitic worm – change their normally cautious behavior by frequently surfacing and flipping over to reveal their shiny silver bellies. This increases the chances of predation by seabirds – by a factor of thirty – ensuring that the worm is passed on to the bird vector.9 Shaw, the parasitologist leading the study of killifish, concludes that a drop in serotonin raises levels of aggressive behavior, whilst a concomitant rise in dopamine makes them more restless. Together, an effect is produced whereby infected fish “display four times as many conspicuous swimming behaviors as uninfected ones”.10

All of these are examples of very profound behavioral changes. In terms of maintaining my analogy, my contention is that a package of ideas (memes) could exercise profound changes if they could produce changes in brain chemistry. We already know both anecdotally

---

and with reference to scientific evidence that what we believe does influence our brain chemistry. Behavior could be modified to, say, become satiated by achieving new objectives, alter perception of risk and pursue a radically different lifestyle. Many of us force such changes when we undergo some lifestyle modification (e.g. giving up smoking; deciding to lose weight; acquiring qualifications and a radically different career). We could, therefore, be said to be actively self-infecting ourselves with alternative sets of memes.

Sometimes these are effective and ‘stick’, other times less so. I am not claiming that there is any likelihood that those who become infected with pro-suicide bombing (or similarly deviant ideas) are necessarily any different from the rest of us. However, there may well be contextual factors which make it more likely that some individuals adopt such bundles of memes than others.

This paper is an outline contribution that sketches initial thinking in an effort to stimulate responses to enhance and focus my further work in this area. Given that a great deal of terrorist (and terrorist-sympathizer) recruitment and handling is undertaken using ‘cyber’ means (in other words, any form of communication depending on the mediation of computers), the analogy of parasitic infection seems to ‘fit’ with the speed with which individuals can apparently become committed to a violent cause.

In terms of further thinking, the following topics (among others) suggest themselves to me as being worthy of further consideration, not least by looking into analogies of terrorist recruitment and self- / group-reinforcing actions in, for example, workplace deviant behavior:
What can we speculatively consider might be the effects and causes of other neurochemical effects?
What changes on perception and behavior might we explore?
In what ways might changes in emotional state be achieved?
What further insights might we analogically explore from animal models?
How might we understand and model the ‘lifecycle’ of infection by memes which shapes information-seeking and satiation but is still far from connection to active pursuit of violence and self-sacrifice?
What can we learn for individual / systemic counter-radicalization from the responses of biological systems to parasitic infection?
What might be the contextual (genetic?) predispositions and conditions that make people susceptible to infection by memes which contribute to achieving deviant behavior?

V. CONCLUSION

This paper set out to demonstrate solely that there may be some benefit in exploring a biological analogy for the future better understanding of the recruitment and motivation of suicide terrorists. The author has identified some potential value in the benefits of a radically different perspective to conceptualizing the mechanisms and individual effects and benefits of radicalization. From applying this biologically-inspired approach, it is hoped that new and innovative concepts for application in policy, doctrine and operations will be produced. Further strands of research and development have been identified and collaboration with other scholars and practitioners is actively welcomed.