Shaping Preventive Policy in “Cyber War” and Cyber Security: A Pragmatic Approach

Tony Guo, University of Miami

Available at: https://works.bepress.com/tony_guo/2/
Introduction

On January 28th, 2011, Egypt disappeared from the global map. In a coordinated shutdown of all major Egyptian internet service providers—an effort by its government to squelch public dissent—virtually all Egyptian Internet addresses became unreachable worldwide. The action was unprecedented in Internet history. At the same time, the U.S. Senate introduced a bill that would give the President the same power to shutdown “critical” Internet infrastructure in the event of a “national cyber emergency.” This bill and others like it were introduced in light of the political rhetoric on “cyber war.”

In recent years, “cyber war” has emerged as one of the nation’s most widely publicized national-security concerns. “In the past, you would count the number of bombers and the number of tanks your enemy had. In the case of cyber war, you really can’t tell whether the enemy has good weapons until the enemy uses them,” says Richard Clarke, former chairman of the White

---

1 J.D. University of Miami School Of Law. B.S. Computer Engineering, Purdue University. I may be reached at tony@tonyg Guo.com.
3 See Id.
House Critical Infrastructure Protection Board. In his recent book, *Cyber War*, Clarke forecasted that an offensive cyber war on the United States might result in the following:

> Within a quarter hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting toward Wilmington and Houston. Refineries are burning up oil supplies in several cities. Subways have crashed . . . [f]reight trains have derailed . . . [and] aircraft are literally falling out of the sky as a result of midair collisions across the country. . . . The financial system has also frozen solid . . . . Several thousand Americans have already died.

Former Vice-Admiral John Michael McConnell echoed similar warnings, stating that “the United States is fighting a cyber war today, and we are losing” because “our cyber-defenses are woefully lacking” and “we have not made the national commitment to understanding and securing cyberspace.”

Clarke is currently a Managing Partner at Good Harbor Consulting, a firm that advises governments and companies on cyber security and other issues. McConnell is now Vice Chairman of Booz Allen Hamilton, a defense contractor that recently landed a $34 million cyber contract, $14.4 million of which was required to build the recently completed United States Cyber Command (CYBERCOM). CYBERCOM was officially activated on May 21, 2010 and announced its first commander, Army General Keith Alexander, who made it clear that he wants more access to e-mails, social networks, and the Internet in order to protect America and

---

7 Id. at 67.
fight in what he sees as the new warfare domain, cyberspace. The federal government currently spends $6-7 billion annually on unclassified cyber security work, and pundits have criticized that Clarke, McConnell, and others have been using the national limelight to create what has become a military-cyber complex.

The recent proponents of “cyber war” may have profitable motives, and there is no evidentiary basis that cyber warfare has ever been waged, or will be in the immediate future. However, American security officials for the most part agree that cyber security is highly relevant to national security, and it is theoretically possible that a foreign military or an independent hacker could be capable of creating a degree of chaos in the United States. These fears, however, may have been exaggerated. Some argue that the confusion in terminology has led to a belief that cyber war is already here, and the real danger lies in the difficulties of holding the military back from infringing on our civil liberties.

This article attempts to provide a cogent analysis of “cyber war,” cyber security, and preventive policy. It argues that “cyber war” is not “war,” and the laws of warfare do not apply. Cyber war is an issue of security—systems security, network security, and due diligence on part of its operators—the legal responses considered should be limited to such. Part I will draw distinctions in cyber security, specifically between attempted definitions of “cyber war,” cyber espionage, and related terminology. Part II will explain the difficulties of applying law on warfare as a deterrent, and why “cyber war” should not be considered as war. Part III argues that “cyber war” is an exaggerated hypothetical, and most security breaches today are issues of poor

---

14 See Id.
15 See Id.
systems security and human error. Lastly, Part IV outlines some past and present legal responses, and what they might mean to all Internet users in the future.

I. Definitions and Terminology

John Keegan, in *A History of Warfare*, stated that “war” is a “universal phenomenon whose form and scope is defined by the society that wages it.” If war is an evolving concept with no set definition, then how do we define cyberwar? Does it even exist? Despite the attention on the defense departments over cyber security in recent years, an entry for the term “cyberwar” is still missing from the Department of Defense’s Dictionary of Military and Associated Terms. Although an official definition is missing, several others exist.

In Clarke’s book, *Cyber War*, cyberwarfare is carefully defined as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.” The Economist has coined cyberwar as “war in the fifth domain,” and as a doctrinal matter, the Pentagon has “formally recognized cyberspace as a new domain of warfare...just as critical to military operations as land, sea, air, and space.”

A concrete definition is important for legal consequences. For instance, a cyber attack that hacks into a corporate website and defames it is not an act of war, domestic criminal laws would apply, and full Constitutional rights would be enforced. On the other hand, a cyber attack

---

with real, physical repercussions, such as blowing up an oil pipeline, is a use of force, and the perpetrators might be dealt with as enemy combatants.\footnote{Whether the perpetrator would be classified as an enemy combatant would also depend on citizenship, the locus of capture, and the place of detention. \textit{See}, e.g., Rumsfeld v. Padilla, 524 U.S. 426 (2004), Boumedine v. Bush, 553 U.S. 723 (2008), Hamdan v. Rumsfeld (2006), 548 U.S. 557, and Al-Marri v. Pucciarelli, 543 F.3d 213 (2008).}

Richard Clarke’s definition of cyber war does not make war sound so bad: an act by one nation-state to penetrate another’s networks for purposes of causing damage or disruption. Under this definition, a single act by a foreign national—assuming it could be attributed to that state—to defame the United States Parks and Recreation website would be for all purposes, an act of war.

Despite war being an evolving concept, in most of our minds it elicits images of the beachfront of Normandy, of kinetic weapons, loud explosions, mushroom clouds, and a high degree of mortality. Today, the term “cyber war” has been thrown around loosely in the media. It has been a catch-all phrase, used to refer to everything from purely financial crimes to network attacks with physical manifestations that could kill people.\footnote{Jordan Robertson, \textit{Experts question use of ‘cyberwar’ for misdeeds}, ASSOCIATED PRESS, May 5, 2010, available at http://www.msnbc.msn.com/id/36969943/ns/technology_and_science-security/}

Scott Charney, Microsoft’s Vice President of Security, has proposed to categorically separate different cyber threats, so governments and organizations are able to think and respond differently to varying degrees and types of cyber attacks. He named three distinct areas, not to be confused with cyber war: (1) conventional cyber crimes - cases where computers are targeted for traditional criminal purposes, i.e. financial fraud; (2) military espionage - allegations that one nation-state intrudes into and captures sensitive military data of another; and (3) economic espionage – one nation’s support or failure to condemn its indigenous industries from stealing the intellectual property of another nation-state.\footnote{Scott Charney, \textit{Rethinking the Cyber Threat}, MICROSOFT (2009), available at http://go.microsoft.com/?linkid=9729572.}
A fourth category, or perhaps a subcategory under conventional crimes, has emerged again recently under the public eye, “hacktivism.” After the arrest of WikiLeaks founder Julian Assange, hacktivism was used as a form of protest. From prison, Assange proclaimed that “Visa, Mastercard, PayPal, and others are instruments of US foreign policy,” and soon, widespread disruption followed after a hacktivist group disseminated tools to aid in the DDoS attacks on the websites of MasterCard, Visa, and PayPal. 1.3 million Gawker users passwords were also compromised, and Gawker’s Twitter accounts were hijacked to publish messages supporting WikiLeaks.

Unlike espionage, cyber war involves the penetration of foreign networks for purpose of disrupting or dismantling those networks, and making them inoperable. However, quantifying and attributing the threat remains a challenge. First, in quantifying the threat, what amount of damage, or what length of disruption, is required to render a network “inoperable?” Where do we draw the line to distinguish between a cybercrime, such as DDoS hacktivism, vs. cyber war? Second, what degree of attribution is required before we “go to war,” in an interconnected world where any individual might remotely control thousands of other networks from a terminal anywhere in the world?

---


26 Thousands of users downloaded the Distributed Denial of Service (DDoS) programs, which is an attempt to make intended to render computer resources unavailable to its users, whereby, thousands of computers bombard the targeted network with so many requests that it cannot respond to legitimate traffic. See INTRUSION DETECTION FAQ: DISTRIBUTED DENIAL OF SERVICE, SANS INSTITUTE, http://www.sans.org/security-resources/faq/trinoo.php (last visited Jan. 10, 2011).


28 Id.

In addressing these difficulties, Charney laid out six specific factors to consider: (1) many actors; (2) many motives; (3) indistinguishable attacks; (4) shared and integrated structure; (5) unpredictable consequences; and (6) potentially disastrous impact.\(^{30}\) Because the Internet is a shared and integrated domain, it would be difficult to separate military and civilian targets, and the risk of casualties to non-combatant property would be significant and hard to predict.\(^{31}\) Furthermore, society today is redefining “warfare” asymmetrically, characterized by low-intensity conflicts, and a nation-state might often find itself “at war” with a single individual.\(^{32}\)

Does “cyber war” exist, or is it mere fear mongering? Former White House Cybersecurity Coordinator, Richard Clarke, believes so. He believes that a cyber attack could occur at anytime, anywhere, and severely cripple the nation’s infrastructure. His successor, Howard Schmidt, takes a different tone. He says that there is no cyber war, cyber warfare is a terrible metaphor, and there would be no winners in an environment where the world is so interconnected and share the same underlying domain.\(^{33}\)

Whether cyber war exists depends on the definition we give it, but it is not simply a matter of semantics, because it determines how governments prepare and respond to various threats. It is important to keep in mind that warfare in the context of cyberspace should not be easily analogized to traditional kinetic warfare, and that existing international law does not have the foresight to encompass the asymmetrical shift towards low-intensity conflicts from a wide range of anonymous attackers inspired by unknown motives.


\(^{31}\) See Id.

\(^{32}\) Id.

II. “Cyber War” is not War

Existing international laws governing warfare prohibits a state from the “threat or use of force” against another state. 34 Two exceptions exist to this prohibition: (1) actions sanctioned by the Security Council in response to a “threat to the peace, breach of the peace, or act of aggression,” or (2) acts of self-defense in response to an “armed attack.” 35 A typical cyber attack is unlikely to meet a threshold of “force” or “armed attack” to justify retaliatory action, and under the current internet framework, an attribution that the attack was performed by “another state” is near impossible where any actor can act from anywhere with unknown motives. The issue lies not in the law, new treaties and refined definitions will not obviate the eye-for-an-eye framework of international laws on warfare, which presupposes the clear identity of an aggressor and the defined scope of aggression.

Accurate traceability of a cyber attack is difficult, sometimes impossible, in the current Internet environment. 36 Unlike the telephone system, which required tracking and billing capabilities, the Internet was not designed for tracking or tracing the behavior of its users. 37 Originally, the Internet was designed to harbor and facilitate collaboration between communities of researchers, and the tracking of benign users was never a consideration. In fact, one of the original goals of the Internet was that the network be robust and survive in case of accidents or physical damage to the routing infrastructure. Thus, there are many alternative paths to a destination, and packets 38 are automatically rerouted when the most direct path is not available. 39

34 See U.N. Charter art. 2.
38 Data is sent across networks on the Internet via IP packets, each packet contains the data to be sent, the source address, the destination address, a port number. Ports represent the type of service offered by a host machine, i.e.
One of the consequences of this design was the lack of authentication for individual IP packets. This means the information found within, such as the source address, can be easily spoofed. For one-way communication, the attacker only needs to modify the source address, but the attack will be “blind” since the attacker is unable to see the replies sent to the spoofed address. A two-way communication attack is more difficult, but still possible. The attacker has to be connected to the same local network as the spoofed source address, and can use tools to sniff the reply packets as they travel to the spoofed source from the gateway router. Another way to hide the origin of an attack is to use a series of intermediate hosts, also referred to as a “packet laundering” technique. By using a large number of intermediaries, this technique is very effective in thwarting trace back attempts when there are significant time delays between attacker activities.

Under current conditions, cyber crimes, cyber espionage, and other attacks can be directed remotely, with the perpetrator’s identity and location hidden. To address this problem, former Vice-Admiral and current Vice Chairman of Booz Allen Hamilton, Michael McConnell, advocated for re-engineering the Internet:

> We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options — and we must be able to do this in milliseconds. More specifically, we need to re-engineer the Internet to make attribution, geo-location,
intelligence analysis and impact assessment — who did it, from where, why and what was the result — more manageable.\textsuperscript{46}

McConnell further suggested that the technologies were “already available from public and private sources” and can be “further developed to build them into our systems, and into the systems of our allies and trading partners.”\textsuperscript{47} The immediate effects are clear: an undertaking would fuel billions into the military’s black budget and billions more to their private contractors. Existing network technology may become obsolete, and increased transaction cost of new infrastructure will bar many private entities from market. Activity of any user can be pinpointed—what was downloaded, what might have been said, what search terms were used—in case of an “attack.” The perceived dangers may have merit, must be weighed against the economic harms and infringements on civil liberties.

III. Reasonable Cyber Security

“Cyber war” today exists only in the hypothetical, and its disastrous impacts are often exaggerated. For instance, the Estonia incident is a commonly cited example by proponents of “cyber war,” where a number of Estonian government websites were temporarily disabled by angry Russian citizens.\textsuperscript{48} A crude distributed denial of service (DDoS) attack was used to temporarily keep users from viewing government websites.\textsuperscript{49} To borrow an analogy, the attack was akin to sending an army of robots to board a bus, filling the bus so that regular riders could


\textsuperscript{47} Id.


not get on.\textsuperscript{50} A website would fix this the same way a bus company would, by identifying the difference between robots and humans, and preventing the robots from getting on.\textsuperscript{51}

A following MSNBC article dressed up the Estonia incident and asked the question, could a cyber skirmish lead the U.S. to actual war?

Imagine this scenario: Estonia, a NATO member, is cut off from the Internet by cyber attackers who besiege the country's bandwidth with a devastating denial of service attack. Then, the nation's power grid is attacked, threatening economic disruption and even causing loss of life as emergency services are overwhelmed . . . outside researchers determine the attack is being sponsored by a foreign government and being directed from a military base. Desperate and outgunned in tech resources, Estonia invokes Article 5 of the NATO Treaty -- an attack against one member nation is an attack against all.\textsuperscript{52}

The article claimed that “half of this fictional scenario occurred in 2007.” In reality, a lot less than half of it occurred, most Estonian sites immediately cut off access to international traffic soon after the increased bandwidth consumption, and botnet IP addresses were soon filtered out.\textsuperscript{53} Most of the attackers could not be traced, but one man was later arrested and fined £830 for an attack which blocked the website of the Prime Minister’s Reform Party.\textsuperscript{54}

“Cyber war” has been a source of confusion due to the ubiquitous application of the terminology, inclusive of cyber crimes and cyber espionage. Cyber warfare comes with many faulty premises, for instance, proponents argue that it might allow terrorists to successfully attack a much larger target and do disproportionate damage.\textsuperscript{55} However, the reality is that any sufficiently effective attack will invite disproportionate retaliation.\textsuperscript{56} For instance, one nation

\textsuperscript{50} See Cyberwar Hype, CLASSIC LIBERAL (Mar. 3, 2007), http://the-classic-liberal.com/cyberwar-hype.
\textsuperscript{51} See Id.
\textsuperscript{56} For example, the retaliatory attacks on Afghanistan and Iraq after the incident on September 11, 2001. See generally Matthew J. Morgan, THE AMERICAN MILITARY AFTER 9/11 (MacMillan 2008).
may be able to make the claim that any number of nations is harboring “cyber terrorists” and invoke the right of preemptory self-defense. However, “cyber war” as it exists today is not kinetic warfare and should not be confused with traditional notions of war. “Cyber war” is about how to prevent or respond to a DDoS attack, and how to secure systems and information.

Short of “re-engineering the Internet,” one could simply maintain government networks and critical infrastructure on closed-networks using proprietary software or protocols. If an organization has all its systems on a closed circuit, the only threats left are its users. Recent data suggests that problems of attribution may not be the major issue, but having reasonable security is. For instance, the U.S. Department of Homeland Security recently ran a test in 2011 where staff secretly dropped USB drives and CDs in the parking lots of government buildings and private contractors. Of those who picked up the media, an overwhelming 60% plugged them into office computers to see what they contained. If the drive or CD had an official logo, 90% were installed. “The test showed something computer security experts have long known: Humans are the weak link in the fight to secure networks against sophisticated hackers.”

Moving forward, legislation and international treaties should focus on the immediate concern regarding cyber security, not on hypothetical accounts of “war.” Addressing security is practical--attacks are less likely to succeed on secured systems and networks with diligent operators, especially given that the majority of breaches today are as a result of system failures and employee negligence.

---

58 See Id.
59 See Id.
60 Id.
61 See infra Part IV(B).
A study from the Computer Security Institute (CSI) showed that 64.3% of companies surveyed experienced malware infections, 29.2% experienced denial-of-service attacks, 17.3% experienced password sniffing, and 16% experienced web defacement. Upon further analysis based on an Accenture study on corporate data security, cyber crime was found to be the cause for only 18% of security breaches, while system failure accounted for 57% and employee negligence accounted for 48% of data loss. Many careless individuals are uninformed about techniques used to compromise information, such as phishing. Although organizations have written guidelines on internal security protocols, they fail to enforce them, and employees are often unaware of policies that, for instance, prohibit them from taking laptops home or from inserting media drives into their work computers. Perhaps the most effective defense against “cyber war” is increased due diligence, better IT training, and improved security measures, especially given that approximately 85% of critical network infrastructure is privately owned.

According to Howard Lipton from the CERT Coordination Center, “[p]erhaps the greatest threat to the Internet today is the abysmal state of security of so many of the systems connected to it.” One problem lies with commercial off-the-shelf software where the number of features and time to market outweigh the security design, and new vulnerabilities are

63 Creating a culture of caring regarding data privacy and protection, Accenture (Apr. 27, 2010), https://microsite.accenture.com/dataprivacyreport/Pages/default.aspx.
64 Phishing is the act of sending an e-mail to a user falsely claiming to be an established enterprise in an attempt to scam the user into surrendering private information, such as a login and password. See WHAT IS PHISHING? – A WORD DEFINITION FROM THE WEBOPEDIA COMPUTER DICTIONARY, http://www.webopedia.com/TERM/P/phishing.html (last visited Jan. 4, 2011).
65 See Id.
continuously found in most new software. Widespread use means that one exploit could be targeted at millions of systems that have the vulnerable product installed, and a lack of security expertise by most Internet users means that vendor security patches will not be timely installed. As a result, these systems are easily compromised by attackers, who may then use the systems to launch additional attacks against better-protected systems, and to hide the source(s) of the attack.

The expertise of the average systems administrator has also continued to decline. In the early days, a relatively small number of systems were attached to the network, which were administered by individuals possessing the skill required to configure and maintain basic system security. Today, the growing numbers of systems attached to the Internet are operated by users with little or no security or administrative expertise, such as the majority of ordinary consumers who own a PC or Mac. These machines become easy prey for attackers. Furthermore, the Internet today has become decentralized, channeling across international boundaries and countless administrative domains, and there is no uniform monitoring system, or a central administrative control. In the absence of cooperation, there is no global visibility, because no entity can monitor or trace outside of its own administrative domain.

**IV. Legal Responses**

Cyber security legislation is a double-edged sword, on one side it purports to mitigate lost revenue due to cyber attacks; on the other it will increase transactional costs associated with
online businesses, which may bar smaller entities from market entry. In 2010, the Internet economy accounted for 4.7% of the United States GDP, and 5% of all retail sales.\(^{77}\) The Internet contributed more as a percentage of America's GDP than traditional industries such as information and technical services, construction, education, agriculture, entertainment, and recreation.\(^{78}\) A growing number of Americans today are making a living online, from small website owners and blog writers who monetize content through ads and affiliate links, to small retailers who utilize a virtual store front to ship goods directly from the warehouse to the consumer. Moving forward, legislators must tread carefully, as any resultant government intrusion will undoubtedly incur a cost.

Of chief concern to both public and private sectors is the need for \textit{reasonable} security, in the form of (1) improved standards for hardware and software systems, and network protocols; (2) improved training and due diligence of operators and employees; and (3) accountability for those responsible for data or security breaches. Secondary, there is also a need for improved coordination, visibility, and shared control of network infrastructure internationally in order to track, respond to, and isolate attacks.

Cyber security has been of concern since the late 90's, and several industry-specific laws have already been passed over the years. The Gramm-Leach-Bliley Act ("GLB") of 1999 requires financial institutions to implement comprehensive safeguards to protect customer information from foreseeable threats in security and data integrity.\(^{79}\) The Federal Information Security Management Act ("FISMA") of 2002 implemented minimum security requirements for


\(^{78}\) See Id.

each federal agency and certification requirements for its contractors.\textsuperscript{80} Internationally, the U.S. signed onto the Council of Europe’s Convention on Cybercrime, a common criminal policy aimed at protection of society against cybercrime.\textsuperscript{81} Specifically it enumerates clear substantive offenses, such as copyright infringement, computer-related fraud, breaches of network security, and child pornography.\textsuperscript{82} Both GLB and FISMA were narrowly tailored, risk-based policies for cost-effective security, and the Convention merely reiterates domestic criminal law on an international stage. However, recently proposed bills—security concerns polluted with the rhetoric of cyber war—seem to have far-reaching effects.

Most controversial was perhaps S. 773, the Cybersecurity Act of 2010,\textsuperscript{83} which purported to give the President authority to “shutdown Internet traffic to and from any compromised federal government or United States critical infrastructure\textsuperscript{84} information system or network.”\textsuperscript{85} “Critical infrastructure” includes sectors of “agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking finance, chemicals and hazardous materials, and postal and shipping,” an exhaustive list spanning across both public and private institutions.\textsuperscript{86} Such language is extremely broad, and gives the executive discretion to flip what critics have dubbed an “Internet kill switch.”\textsuperscript{87} Under heavy scrutiny, the bill ultimately died, but it brought to light existing

\textsuperscript{80} See 44 U.S.C. § 3541, et seq.
\textsuperscript{82} See \textit{Id}.
\textsuperscript{83} S. 773, 111th Cong. (2009). \textit{available at} \url{http://www.opencongress.org/bill/111-s773/text}.
\textsuperscript{84} Being designated as a critical infrastructure also incurs obligations for upgrades and compliance. See \textit{Id}.
\textsuperscript{85} \textit{Id}.
\textsuperscript{86} \textit{Id}.
\textsuperscript{87} State of the Union With Candy Crowley, CNN.com, \url{http://transcripts.cnn.com/TRANSCRIPTS/1006/20/sotu.01.html}
emergency powers conveyed to the president from Section 706 of the Communications Act of 1934, which it purported to limit—an “Internet kill switch” already exists.\textsuperscript{88}

Section 706 expressly provides that “[u]pon a proclamation by the President that there exists war or threat of war, or a state of public peril or disaster or other national emergency,” the President, “in the interest of national security or defense . . . may cause the closing [or use] of any station . . . or device . . . upon just compensation to the owners.”\textsuperscript{89} The President may also amend or suspend the rules and regulations applicable to “any or all facilities or stations within the jurisdiction of the United States.”\textsuperscript{90} This power applies to both “radio communication” and “wire communication,”\textsuperscript{91} defined as “transmission of writings, signs, signals, pictures, and sounds of all kinds,” as well as all things “incidental to such transmission.”\textsuperscript{92} Although it is difficult to argue that Congress had the Internet in mind when they passed the legislation over 70 years ago, the language seems to encompass all Internet infrastructure. Herein lies the danger of confusing issues of cyber security with war, “war” authorizes the President to take property.

What would a “shutdown of the Internet” mean? Is it even possible? Although the “kill switch” rhetoric might be overblown, the damage would still be severe. Simply stated, the Internet cannot be shut down because of its decentralized characteristics.\textsuperscript{93} The President would however, be able to take segments of the network off the Internet. What would likely happen, in the event of an attack of sufficient degree, is that an administrative official will instruct an operator to block certain incoming packets from certain source addresses, or perhaps temporarily, to block all incoming addresses. Fortunately, two limitations on the 1934 Act exist

\textsuperscript{88} http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MinorityNews&ContentRecord_id=66a8ffe3-5056-8059-765f-7bc7bffed0b2&IsTextOnly=False
\textsuperscript{90} Id.
\textsuperscript{91} See Id.
\textsuperscript{92} See Comm. Act 1934 Sec. 3
\textsuperscript{93} See infra Part III(A).
to protect consumers and businesses: (1) the power can only be exercised in an emergency; and (2) just compensation would be required for any downtime. The Cybersecurity Act of 2010 had no such restrictions.

Recently, the Cybersecurity Act of 2012 has been reintroduced, without the kill switch provision. However, this bill introduces new privacy concerns, for instance it allows any private entity to “monitor information systems,” “operate countermeasures,” and to “disclose any cybersecurity threat indicators” to any other private entity. “Cybersecurity threat’’ is defined as “any action that may result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system” (emphasis added). The language of course, is intentionally vague, and basically allows any one of CYBERCOM’s private contractors to freely monitor and share any online activity of any online actor.

Unfortunately, the “cyber war” rhetoric has found its way into an umbrella of other related bills. For instance, the National Defense Authorization Act declared the Internet as an “operational domain” in the war on terror, and includes authorization to indefinitely detain citizens on suspicion of supporting or sympathizing with broadly defined terrorists, as well as anyone who commits a “belligerent act.” Also as part of the bill, the U.S. military now has authorization to conduct “offensive” strikes online, despite there being zero documented hacking attacks on U.S. infrastructure—a recent report that a water pump in Illinois had been destroyed

---

95 Id at 153.
96 Id at 182.
98 See Id at Sec. 1031(b)(2).
by Russian hackers turned out to be a contractor logging in from his vacation, at the request of the water company.99

Conclusion

What is “cyber war?” Does it even exist? The short answer is no, at least not until we start it. The recent hypothetical accounts of cyber warfare have captured attention of the media and harnessed the imagination of Americans. People scare easily, and there is a profit to be made from scaring people. ‘Cyber war’ has been used as a catch-all phrase, commonly confused with cyber crime, cyber espionage, and hacktivism.100

“Cyber war” is not an issue of war, and the laws covering kinetic warfare is an ill fit. All-out cyber warfare between nations is science fiction, in a world where we all share the same underlying domain, and are all dependent on the same global economy. Instead of authorizing armed attacks in response to imagined cyber threats as a deterrent, attention should be focused on prevention through reasonable cyber security.

Today, the majority of critical network structure is privately owned, and in reality, disruptions, loss in data, and security breaches are mostly the result of human error, hardware failures, abysmal network and system security, and the lack of network visibility.101 Preventive security does not require a “re-engineering” of the Internet, and care must be taken to preserve its openness, which created an expanding culture for innovation in the arts, sciences, and technology. Moving forward, legislators must tread carefully, because any resultant government intrusion will undoubtedly incur a price. Legislators will have to weigh the incremental benefits

100 See supra Part I(B).
101 See supra Part IV(B).
in security against the cost incurred on the private sector, as well as refine the legislative language, since its broad brush will affect everyone and everything on the Internet.