The Report Committee for Jonathan Iming Lee

Certifies that this is the version of the following report

Evaluating Cyber War

APPROVED BY

SUPERVISING COMMITTEE

Supervisor: _____

R. Harrison Wagner

_____

Peter Trubowitz

Evaluating Cyber War

by

Jonathan Iming Lee, B.S.

Report

Presented to the Faculty of the Graduate School

of the University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Arts

The University of Texas at Austin

December 2010

Evaluating Cyber War

by

Jonathan Iming Lee, M.A.

The University of Texas at Austin, 2010

SUPERVISOR: R. Harrison Wagner

Richard A. Clarke and Robert K. Knake's book, *Cyber War*, claims to identify a new threat and vulnerability in the United States. By examining the points they make and evaluating them in the context of the first cyber attack, STUXNET, we shall conclude that the technical argument is correct; however the overall argument is incomplete. What they fail to emphasize is the amount of human intelligence involved in committing a successful cyber attack, and the extent to which having intelligence operations greatly enhances a state's cyber capabilities.

Table of Contents

Introduction

Richard A. Clarke became a household name in the aftermath of September 11th 2001, when it was revealed that his warnings about an Al-Qaeda attack of such a scale had gone unheeded across two Presidential administrations, and that he himself was marginalized in the twilight years of his civil service. Upon completing his 30 years in the government, he graduated in typical fashion into private consulting. In early 2010, Harper Collins published his highly anticipated book, which was coauthored by Robert K. Knake, that documents a new warning: *Cyber War: The Next Threat to National Security and What to do About It*.

First, a definition and a short summary: as Clarke and Knake describe on page 3, "when the term 'cyber war' is used in this book, it refers to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." Clarke and Knake are not talking about mere espionage, but counterforce and countervalue. In summary the authors are making these three points: 1) that cyber warfare is possible and upon us, 2) that the United States is particularly susceptible to cyber attack, and 3) that there are steps it could take to mitigate its susceptibility to cyber attacks.

With the benefit of a few months and a few real world incidents, a clearer picture of the reality of cyber warfare has emerged. And with this, a better means to gauge the accuracy of the book. In particular, the STUXNET worm (Zetter 2010, *DEBKAfile* 2010),

commonly viewed as the first wave of cyber attack, could be considered much needed proof that the book could otherwise not provide. However, more than this one example is needed to verify the conclusions of their book; specifically that Clarke's prescriptions are the correct ones to take.

This paper will go beyond the initial evaluations by critics and supporters, and consider whether Clarke's fore-warnings and conclusions make internal and technical sense. We will discover that while Clarke is actually technically right regarding the vulnerabilities he identifies, his analysis is incomplete. What he misses is the fact that states have other assets, intelligence operations that enhance their ability to conduct cyber attacks, which bypass many of the technical vulnerabilities which are highlighted. His critics are right to challenge his argument, but they also miss this crucial piece.

The Criticisms

Clarke's introduction to the problem of cyber warfare is a sneaky one. The book opens with a rather colorful anecdote from 2007 about Israeli fighter-bombers destroying a Syrian nuclear reactor site in a daring midnight raid. But beneath this depiction he pulls at an unnoticed thread, at how these stealthless fourth-generation aircraft overcame a sophisticated air defense system designed precisely to counter this type of attack. The Israeli Air Force had hacked the Syrian defense networks and had co-opted the radar system to read clear skies. In this way, Clarke introduces cyber warfare as the shadowy counterpart to direct military action. He tries to inform his reader of the threat posed by something that is essentially invisible, by pushing it into the light of an exploding nuclear reactor.

Yet within a matter of pages he commits a glaring technical blunder: he conflates radar signal with data packets. There is no mistaking author's intention, as the writing is very specific in the text of the error on page 7:

> A stealthy Israeli UAV might... have been able to detect the radar beam coming up from the ground toward it and used that *very same* radio frequency to transmit computer packets back down into the radar's computer and from there into the Syrian air defense network. [Emphasis added]

If we take the authors' claims seriously, then we would be led to believe that Syrian radars are blanketing the sky with radio waves of the exact same frequency used by

their communications network, in the exact same waveform as a typical data packet of headers and information. Further, a careful reader might have noticed this preceding passage on page 6: “Radar still works essentially the same way it began seventy years ago at the Battle of Britain. A radar sends out a directional radio beam. If the beam hits anything, it bounces back to a receiver.” Thus at least one of the authors has some idea about how radar works. Perhaps Clarke really meant to say that the stealth UAV flew in to discover the defense communications frequencies, gather some wireless traffic, send that home, and have machines break the encryption, all done days in advance. Or perhaps they simply jammed the radar site, or otherwise spoofed the radar using software similar to Suter (a BAE software package designed specifically to defeat air defenses). Regardless, the language very clearly communicates a technical error to the reader very early on in *Cyber War*.

This point is completely missed in all the reviews of his book, some of which are very skeptical and others outright critical of Clarke's message. How is it that these reviews, which claim to identify Clarke's misunderstandings on technical matters, neglect to point out a technical blunder that is so easily noticed on page 7 of the book? Did they even read the book, and what is the critique that they present? I’ll provide three representative examples:

First, Michiko Kakutani (2010) from *The New York Times* makes little attempt to evaluate statements made in the book, instead relying on Clarke's credentials as the misunderstood counter-terrorism chief to two Presidential administrations, and his “insider’s knowledge” as reason enough to accept the portents and solutions presented in *Cyber War*. Second, Misha Glenny (2010) from the *Financial Times* attempts to write a balanced piece, closing with the sentiment that “the truth lies in between;” however a

quick read and word count will betray a not-so-subtle critique of academics, civil servants and security professionals seeking federal funding, and an emergent "cybersecurocracy" securing little beyond government bloat. Third, Evgeny Morozov, a contributor to *The Wall Street Journal* and *Foreign Policy*, has been openly critical, although he hasn't directly reviewed the book. He writes: "Wired says Richard Clarke's Cyberwar should be filed under fiction. I say science fiction," and "given that Clarke runs a cybersecurity consulting firm, what else would he say? That America's cyber-defenses are secure?" (I will discuss the *Wired* review shortly.) There are others, including ones in *The Wall Street Journal* (Reynolds, 2010) and *The Washington Post* (Stein, 2010), which fall into one of these general categories.

Essentially these are ad hominem attacks on the authors, rather than evaluations of their argument. While they claim to point to Clarke's failings in technical sophistication (and the authors admittedly chose to write for a non-technical audience), they aggressively paint Clarke as an opportunist seizing upon his new-found fame as a prophet of national security. In other words, he is a super-mutant variety of the government employee cashing out as a private contractor, writ large. On the other hand, the piece in *The New York Times* doesn't properly address the book's content either, relying on the reputation of the author as sufficient, thereby merely accepting an argument from authority. Neither approach addresses the authors' argument directly.

The merit of evidence is measured by the credibility of its source, while merit of an argument is measured by the quality of its logic and assumptions. For example in *The Wall Street Journal*, Evgeny Morozov rightly dismisses the "simulation" concocted by industry insiders and broadcast on CNN (16 February 2010) dubbed "Cyber ShockWave" as fear-mongering. This demonstration via a fishbowl simulation of

American vulnerability to cyber attack, performed by security and policy firms, cannot be considered credible evidence of an actual vulnerability. However, Clarke's *Cyber War* is simultaneously a testimony and an argument: he recounts his own experiences in government on national cyber-security issues, but he also assembles an argument about this next-generation threat. This argument deserves a fair evaluation.

The most provocative and promising critique of Clarke's book comes from *Wired*'s review "File under Fiction" by Ryan Singel (2010). He first states that much of the book could "easily debunked with a Google search, or so defies common sense." And he justifiably complains that the author provides absolutely no footnotes, endnotes or bibliographical entries, sardonically adding "Revelation doesn't need sources." Apparently neither does the contentious book review. While the article poses actual direct counters to the book's main points, there are no notes or hyperlinks to sources in his refutations; it's his word against Clarke's. What exactly we are meant to debunk via Google search and what we are meant to assume as nonsensical is left unexplained. He rounds the review by repeatedly poking fun at Clarke's allusions to Hollywood movies and ridiculing the silliest examples from the book (throwaway examples such as photocopiers exploding) as examples of the fantasy engendered by *Cyber War*.

However, this does point to several poor choices in the book's writing. In addition to lacking notes and references to sources, there are various points where he could have anchored his points with straightforward summaries or conclusions, but instead chooses parochial punchlines to conclude otherwise serious points. At one point he even preempts criticism by stating "quibblers will argue with the overly simplistic methodology" when presenting a chart filled with numbers representing "cyber war strength" on page 148. (I'll quibble: The numbers aren't even derived from anything. They are simply his

own estimates; in which case a scale like “high,” “medium,” and “low” should have sufficed. Still worse, he concludes from the numerical chart that “the results are revelatory.” Thus he declares revelation from numbers he had literally made up!) While this is more an issue of style, it is in the book and it does detract from the reading.

In the end, Clarke and Knake are making serious claims. Except they do so in a book appealing to a wide audience, rather than technical experts. They intend to motivate a non-expert public into being concerned with a technical problem that is impossible to visualize, doing their best with analogs and description (see Appendix I: The Political Context). And this rhetorical strategy can be easily dismissed as fear-mongering, especially coming from an individual who had just made the jump into the private security consulting. Eisenhower's old warning about the military-industrial complex echo loudly while reading. However, the claims are broad, and if true, the consequences are severe. The argument should not be read lightly.

The Argument

As stated in the introduction, the book can roughly be broken down into three points: 1) that cyber warfare is possible and upon us, 2) that the United States is particularly susceptible to cyber attack, and that 3) there are steps it could take to mitigate its susceptibility to cyber attacks. Clarke and Knake's *Cyber War* consists of eight chapters: Chapters Three, Five and Eight make up the bulk of the technical argument and solution.

Chapters One and Two introduce the topic, provide definitions and go over who's doing what in cyberspace, specifically the US, North Korea, China and Russia.

Chapter Three begins the heart of their argument, where the authors go over the technology and its vulnerabilities: 1) the structure of the Internet backbone, its openness and commercial penetration; 2) the routine bugginess of both software, which is growing increasingly complex with line-counts in the millions, and hardware, which is predominantly manufactured overseas; and most importantly 3) SCADA systems. Defined on page 98 as "Supervisory Control And Data Acquisition" systems, SCADA systems are the means by which real-world systems such as transit controls, utility pipelines, and electricity are monitored and routed, remotely via computer controls. (An example is the Siemens industrial control software targeted by STUXNET.) These points will be examined more closely in the next section.

Chapter Four reviews Clarke's allegations of neglect by Presidents Clinton, Bush and Obama. Each time Clarke was greeted with warm enthusiasm and initial readiness to engage, but he found that the various Presidents would in-turn defer to large political donors. Further, the chapter explains that the NSA and Department of Defense are responsible for defense networks and offensive capabilities, Department of Homeland Security covers government networks in general, but no government entity has responsibility for the private Internet.

Chapter Five returns to the argument, and suggests a three pronged strategy to handle the cyber-vulnerability of the American public. First, the Internet backbone should scan traffic for malware signatures; second, America should black-box or air-gap the power-grid specifically; and third, America should enhance the security of its classified military networks.

Chapters Six and Seven branch out to broadly cover classic political science concerns: escalation, retaliation and military strategy, diplomacy and geopolitics, and then a follow-on chapter on arms control and use limitations. Given the lack of agreement on the exact effects of cyber warfare, these points appear premature and underdeveloped.

Finally, Chapter Eight concludes the book, summarizes the broad points and provides a six-point agenda that should guide American thinking about cyber-warfare for the long term. From the points scattered across these chapters, the following premises can be constructed:

1) States are willing to exploit cyberspace. They are interested in attacking SCADA and other systems and have done so, and since the Internet is wide open, they can obfuscate the origins of an attack. The book quotes former

Director of National Intelligence Admiral Mike McConnell: “The vast majority of industrialized countries in the world today have cyber-attack capabilities” (p.64). (A side note: they state that Cyber-terrorism is a red herring, as terrorist groups are using the Internet mainly for communications, not attack.)

2) The Internet backbone is unmonitored. Anything can get anywhere by design. The architecture of TCP/IP involves only scanning packet headers for destination information, and thus the gateways and routers blindly forward any traffic as requested: “While the protocols that were developed based on these rules allowed for the massive growth in networking and the creation of the Internet as we know it today, they also sowed the seeds for the security problems” (p.83).

3) SCADA systems, for power, other utilities and transit, are not secured. Attempts to isolate them using virtual private networking and firewalls are imperfect. Most worrisome is that an attack on power is also a simultaneous attack on all the others, including finance, government and military systems, as backup systems are temperamental and unreliable: “These control programs... regulate the electric load in various locations. The signals are most often sent via internal computer network... Unfortunately, many of the devices also have other connections. One survey found that a fifth of the devices on the electric grid had wireless or radio access... and almost half had direct connections to the Internet” (p.98-99).

4) While USCYBERCOM/NSA has the military covered, Dept. of Homeland Security has the civilian government covered, no one has the U.S. private sector Internet covered: “U.S. Cyber Command also has a defensive mission... the Department of Homeland security defends the non-DoD part... There is no

federal agency that has the mission to defend the banking system, the transportation networks, or the power grid" (p.143). Further, civilian Internet security isn't even regulated: "the Federal Communications Commission has the legal power to regulate but it largely chosen [sic] not to do that" (p.146).

5) The United States is more dependent on the Internet than its closest global competitors, particularly in having its infrastructure reliant on networked computer controllers: according to Clarke's testimony, the US is the most "reliant upon networks and systems that could be vulnerable to attack" (p.148).

6) Even without immediate access, a state could implant logic bombs to destroy precious data or pre-position backdoors to exploit at sensitive times: "The phrase 'preparation of the battlefield' has become somewhat elastic. The battle does not need to be imminent, and almost anyplace can be a battlefield someday..." "[Installing trapdoor or logic bomb] does not mean that you have already decided to conduct that war, but it certainly means that you want to be ready to do so" (p.198-199).

7) Finance is vulnerable, and while it should be secured, it is slightly less of a concern (as compared to SCADA systems) because states' financial systems are interdependent and governments don't wish to see banking institutions involved in fighting: "Every major nation has a stake in the reliability of the data that underpin international bank clearing houses... a cyber attack on one nation's financial infrastructure could have a fast moving ripple effect, undermining confidence globally" (p.246).

In short, the U.S. is most highly wired and networked, with critical systems vulnerable due to their inadvertent accessibility via the Internet, threatened by capable states that indeed have plans to exploit such vulnerability for political reasons.

From these premises he concludes 1) cyber war is possible and can generate real world effects 2) that the United States is ultimately the most vulnerable power in cyberspace, 3) since reacting to an attack is essentially impossible, we can best overcome these problems by prevention and preparation. Of course there's far more going on in the book: Clarke's experiences in government, detailed histories of the various efforts being made by each nation, and more. However these other points rely on this central piece working correctly. These premises and conclusions lead them to propose three solutions in Chapter Five:

> 1) Have the major tier 1 ISPs scan the Internet backbone for digital signatures of an attack using existing technology: "If you could catch the attack entering the backbone, you could stop it before it got to the network it was going to attack. If you did that, you would not have to worry as much about hardening tens of thousands of potential targets for cyber attack" (p.161).
>
> 2) Secure, or air-gap the power-grid: "Without electricity, most other things we rely on do not work, or at least not for long. The easiest thing a nation state cyber attacker could do today to have a major impact on the U.S. would be to shut down sections of the Eastern or Western Interconnects, the two big grids that cover the U.S. and Canada" (p.167).
>
> 3) Secure the nation's defense networks, NIPRNet (unclassified), SIPRNet (secret), and JWICS (top secret): "if an opponent were going to hit us with a large cyber attack, they would have to assume that we might respond kinetically. A

cyber attack on the U.S. military would likely concentrate on DoD's networks" (p.171).

Further, there is his six point agenda in Chapter Eight: 1) enhanced dialogue about cyber war, 2) better regulation to accomplish the above three solutions from Chapter Five, 3) reduce cyber crime, 4) international limits on cyber war, 5) better software, 6) the President should be in more involved.

The next three sections will evaluate the argument and the solutions presented in *Cyber War*. First, we'll assess at how accurate they are about the technical threat. Second, we'll discuss what they should have discussed in greater depth: the human factor and human intelligence in cyber warfare. Third, we'll present a critique of the solutions that are given in the book.

From Bugs to Armageddon

In the 1990s, a considerable fuss was made regarding the turnover to the year 2000. Dubbed the Y2K bug, the concern was that the underlying code upon which banking software, air traffic control systems, and utility management software were built, would crash once computer clocks went from 12/31/99 to 01/01/00. This was a memory saving shortcut from the kilobyte era that was written into software that nobody believed would still be in use 30 years later (and the next time this problem will occur is in 2038 with the UNIX clock bug). When civilization didn't collapse on January 1, and the machines upon which we depend continued to function, the question was raised whether it was all the preparation and prevention that mitigated the effects, or whether the original threat was overblown. There are some parallels between Y2K and cyber warfare.

The Internet grew out of what was essentially a science experiment. The original creators could not have envisioned their project being used in such a fashion, pushing such massive volumes of data across the globe, with energy networks, financial services and other utilities wholly dependent on it (when a corporate network goes down due to a worm attack, it is an automatic work-stoppage). One example of the Internet as an experiment colliding with its unintended usage is the IPv4 address exhaustion. As the Internet expands, and connected devices proliferate, IP addresses are assigned to each new device. When the Internet was first devised, the creators assumed that, for their

little experiment, 32-bit addressing would suffice (4.3 billion unique IP numbers). Yet decades later these address numbers are rapidly running out, and moving to the new standard, with 128-bit addresses, has caused a small stir with implementation. Every few weeks there is a new story about this migration, specifically with regards to legacy networks, updating ISP routers, and OS tunneling between IPv4 and IPv6.

Here is Clarke's opening salvo in *Cyber War*. He warns that no less than national security is at stake, based upon the combination of the Internet's inherent openness and bugs in the end-users' software. Like Y2K, the Internet's myopic design of convenience has essentially become a bug that, as Clarke would argue, has potentially catastrophic consequences. He identifies five weaknesses in the design of this once experimental Internet: 1) the addressing system (the Domain Name System servers), 2) the routing system (the Border Gateway Protocol system), 3) the fact that the vast majority of traffic is unencrypted, 4) the existence of malware, and the 5) decentralized design (p.74-82).

What we must evaluate is how right Clarke is on these fronts. Regarding the DNS servers, DNS poisoning is a well known attack vector: Clarke provides not only how this is accomplished, he explains its origins also: the security specialist Dan Kaminsky (p.77). This is also a relatively recent discovery (2008) of a latent bug that has existed since the birth of the Internet.

Likewise with the BGP: researchers have handily shown that this is a possibility. Here, adversaries can not only surreptitiously read the traffic, collect it to analyze later, and forward it to its final destination, they can also modify its contents if they had the wherewithal to do so (Zetter 2008). Again, this is an architectural vulnerability that has existed for as long as the internet has.

However it has always been known that the vast majority of internet traffic is unencrypted, and that this poses a severe problem. Running a packet sniffer will display the contents of most data transmissions over any unsecured wireless (e.g. one can use “ethereal,” renamed “wireshark” to do so). Secured wireless has also vulnerable: given time, a machine can collect packets in silent mode, and eventually crack the encryption key (e.g. using “airsnort,” renamed “aircrack”). WPA2 actually has an implementation error such that a man in the middle can read and manipulate traffic without even dealing with the AES encryption it employs (Wexler 2010). What’s worse is that while many password pages do use end-to-end encryption (your email login page with the “https”), the identifying cookie is sent unencrypted. Listening in on the wireless traffic allows an attacker to easily swipe the cookie, and then pretend to be the user (this is in fact so easy, in early 2010 a concerned netizen, Eric Butler, wrote a plug-in for Firefox named “Firesheep,” which can do this automatically for any user, to illustrate why this is a major problem). Telnet, a popular connection protocol, does not even encrypt the password field, such that it can be clearly seen to any listener; Telnet was bundled with operating systems as recent as Windows XP.

Moreover, the computing solutions employed by end users of the Internet, home user operating systems, browsers, browser plug-ins, and middleware (ActiveX, Adobe Flash, Adobe AIR, Java, PDFs and Silverlight), are prone to vulnerabilities. Every few weeks, a new “zero-day” bug is discovered, requiring patching by Microsoft or Adobe on the next “patch Tuesday.” From default open ports in operating systems, the infamous Windows .dll bug, to the Linux kernel’s root-user privilege bug in its 64-bit implementation (which went un-patched for years), the opportunity for malware exists on every single machine connected to the Internet.

His last point about the decentralized nature of the Internet isn't particularly remarkable, except to suggest that any attempts to effect change would involve coordination between a number of entities. He rightly points out that it was precisely this decentralized nature that spurred the explosive growth of the Internet, but there isn't much more here than there was in the first two points regarding the Internet's architecture.

Clarke's next major point about cyber warfare is where cyberspace meets the real world: government command and control and SCADA systems. This is the point where the Internet goes beyond espionage, and into the realms of counter-force and counter-value capabilities, or real cyber war.

First, Clarke points out how the U.S. government has transitioned from the leading edge of computing to the trailing edge. Before, the government had the premier computer scientists and programmers, and military computing operating systems were custom written for government purposes. Now, the vast majority of innovation on this front occurs privately, and for-profit. For example, when I worked for the Air Force Research Laboratory, I visited a start-up technology company in Boston prior to their IPO, and reviewed their technology and funding. When I asked about what their funding levels were and how much more they needed, I was rebuffed: any money I had to work with was dwarfed by what the mobile phone companies were already putting in. Furthermore, software programs that were vital for the war-fighters I was supporting, irreplaceable pieces of kit, were all written solely for the Windows operating system. I recall asking a communications officer, who was part of the team behind the "secured" Air Force specific version of Windows Vista, what we got for our money: he replied "too little for too much."

More importantly, Clarke provides numerous examples of how private industrial SCADA systems are vulnerable (p.96-101). STUXNET puts this into stark relief, when previous occurrences hadn't convinced others, namely when U.S. power facilities were allegedly under threat (Gorman 2009). In particular, the SCADA system specifically targeted by STUXNET had faults shared by other industrial control systems. The Siemens control software packages (WinCC and PCS7) actually required that the passwords be kept to the default value for the control software to properly function. Further, as software packages built for Windows systems, they were subsequently susceptible to any number of zero-day vulnerabilities missed at Microsoft (Falliere et al 2010). And, like all malware, only a small number of tweaks are necessary to target alternative SCADA packages (Clayton 2010).

In short, from a technical standpoint, Clarke had solidly identified areas where the Internet is vulnerable, relying on bugs which had previously been highlighted back in 2008. And in areas where he might have speculated, reality very quickly confirmed the existence of the threat. Like Y2K, much of the Internet's vulnerability is an unintended consequence of a technology outlasting its breadboard origins, of an experiment turned into the basis for modern commerce and communications. Like Y2K, Clarke argues, preemptive measures and prevention are necessary to protect modern society. The bugs in the design are real, in each level that Clarke identifies. However, there's more to cyber war than there was to Y2K: it requires a determined adversary.

The Human Factor

Where Clarke missteps, and where the critics have a stronger case to make, is with regards to human agency in cyber warfare. Clarke was right when he made the point that states are interested in conducting cyber warfare. He is also correct in stating that cyber terrorism is not a major threat, as confirmed by other researchers (Cavelty 2007, Conway 2007).

While he makes these points, he repeatedly slips into a mode of fear-mongering: he'll use the image of faraway hackers and their laptops hiding in a closet, bringing down U.S. systems, one after another, and obfuscating their attack paths through servers in third party countries (p.64-68, p.101). Here, the critics have the most leverage to poke holes in what Clarke is saying: his occasional slips into a simplified caricature of his own points stretch his credibility. Technically he makes sense at every level, from the Internet's open design, to software vulnerabilities, to SCADA under attack. However, his breakdown is incomplete: all the technical reasons together paint a picture of cyber warfare as a sterile attack that can be accomplished across continents by unseen forces. The vulnerability he neglects to include is human failure.

First, human misuse is a major concern: this ranges from weak passwords, poor security practices, and naive online practices, to keystroke logging, susceptibility to phishing and other social engineering. Federal employees bring work laptops home but leave the hard drive data unencrypted; every few months a laptop containing sensitive

data is stolen from a federal employee's car. In Afghanistan, security specialists had to sweep up all the USB keys floating in the marketplace, as many contained sensitive information, and were swiped from military computers and barracks. Even when government directives order USB keys be banned, the ports are left activated. The authors of STUXNET are believed to have gotten intimate details of the Iranian nuclear control systems by accessing the laptop of an Iranian official while travelling overseas.

People reuse the same passwords at work and online. Further, these passwords are routinely very weak: a recent leak of Hotmail passwords revealed that the following passwords were used most frequently: "password," "123456," and "qwerty." Social networking has also opened an entirely new class of online threats that exploit human failures rather than technological ones (Dhanjani et al, 2009; McAfee 2010). If Clarke wished to make the claim that the U.S. is most vulnerable to cyber attack, he should have mentioned the penetration of social networking: Facebook traffic has overtaken Google traffic in North America.

Second, and perhaps more importantly, states and other determined adversaries have methods available to them to shortcut various security measures; skipping over technical obstacles using well placed intelligence operatives or exploiting social engineering as stated above. Clarke makes certain to argue that states and their intelligence agencies are actively engaging in this type of activity but doesn't emphasize enough the fact that these operate in concert with the technological angle. Recall the definition of cyber war: "when the term 'cyber war' is used in this book, it refers to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" -- this does not preclude humans accessing such devices directly.

While Clarke argues that that a hacker can attack from anywhere in the world, the biggest threat still remain the inside man and social engineering. Examples of this include the recent leak of classified documents, taken from the top secret JWICS computer network by Private Bradley Manning. He burned gigabytes of classified data while pretending to listen to Lady Gaga (the jewel case in fact contained the blank DVD media onto which he burned the data). The U.S. secret network was also brought down in a similar way: an authorized individual stuck an infected USB drive into a military computer, specifically a laptop, and the end result was that the classified SIPRNet was breached (Nakashima 2010).

STUXNET is a prime example of this. It is believed that the Iranian nuclear power network was fairly well insulated from the Internet (despite Clarke's assertion that SCADA systems are notoriously unsecured and routinely have their radios misconfigured as on [p98-99]). Security professionals conclude that the worm was likely introduced thought a USB key via intelligence operatives or their contacts. Further, STUXNET highlights the fact that a determined state intelligence agency was interested and capable of conducting such an attack, especially given the quality of the worm, to include multiple zero-day vulnerabilities, and stolen security certificates to run system-level drivers (Falliere 2010).

Inside knowledge of the target system is also clearly apparent in STUXNET: the worm instructed the control numbers, those corresponding to the target centrifuges, to spin up above their breaking point, and the closing command slowed them back down to almost exactly their normal operating frequencies (Clayton 2010).

Perhaps it is in this way that the U.S. is most vulnerable. Traditionally the U.S. intelligence community holds the lead in SIGINT, or signals intelligence, while it had

lagged in the area of HUMINT, or human intelligence. Although Clarke gives an accurate breakdown of the technical vulnerability of a wired nation, he doesn't give enough credit to the human factor in exploiting that vulnerability. The greater distance between a cyber warrior and his target, the more sophisticated he must be to overcome the various layers separating him from that target. Having only a little social engineering or having an inside man cuts the required sophistication dramatically.

Solutions that Make No Sense

Taking Clarke's solutions seriously, we find them disappointing given the technical threat he identifies, or otherwise they are intrinsically underwhelming or obvious. What he lists: scanning the Internet backbone (top tier ISPs) for malware signatures, securing the military networks further, and isolating the power grid, are not bad solutions, however they essentially add little to what is already being done. At worst, they contradict statements Clarke makes earlier in the book. They really aren't solutions at all when looked at closely.

What is likely the most controversial solution, scanning the Internet for malware signatures, is also the most interesting. Clarke's critics consider this the most troubling of his suggestions from a civil liberties point of view, pointing to current bandwidth throttling as a precursor to broad content filtering if scanning is done (Singel 2010). Further, they point to the fact that ISPs already attempt to filter malware on their networks. However, when one also includes the difficulties encountered with regard to the IPv4 to IPv6 transition, adding a thorough packet scanning requirement to the top level ISPs might be overwhelming. On the other hand, Canada appears ready to embrace this approach (Geist 2010).

Again, what this misses is the danger of the inside man and social engineering, which provide alternative vectors of attack and bypass using malware to gain privileged access. Physical access to a USB port is enough to access an air-gapped network as

mentioned above. Social engineering can get a keystroke logger installed on an office machine, though which a hacker can obtain authentic credentials (Dhanjani et al, 2009).

The second solution is, by contrast, overwhelmingly obvious. Further securing the military networks is what he proposes: this is a prescription that no one could possibly disagree with. He provides specific direction regarding low-cost ways to improve the defense network: firewalls, anti-virus, multiple forms of user authentication, segment the networks, encrypt machines, and monitor traffic (p.174). If we accept these as novel recommendations, we'd have to conclude that the U.S. military networks consist of the least secured computers on the planet.

Third, specifically isolate the power grid SCADA, appears to contradict the arguments he had made earlier. His earlier point is that it was essentially impossible to completely isolate a large-scale network. Further, any supposedly isolated SCADA machines were improperly configured 20% of the time (that is, have open connections to the Internet, or otherwise have their wireless radios on), and up to half inadvertently had direct connections to the Internet. Thus this solution is essentially saying 1) his earlier point about network penetration vulnerability can be overcome, and 2) that the network security staff should do their jobs better. So again, we are presented with a non-solution: we need to secure our vulnerabilities.

Clarke goes on to include better regulation (Chapters Four and Eight) as a necessary steps in achieving the three solutions presented above. He cites "smart regulations" several times as a path to achieving cyber security. Again, we have to ask who disagrees with this vague notion of improved regulation (other examples of his long-term solutions from Chapter Eight include reducing cyber crime and improved software).

What Clarke really means in this regard, and he waits to say this at the very end of the book (p.276-279), is that the U.S., very specifically its Executive, lacks the political will to make the necessary demands on private industry: the electric companies and top level ISPs. While the federal government already has the power and regulatory authority to govern the private carriers (p.146), and impose fines on the power utilities (p.100-101), it has not (as evidenced on an entire chapter dedicated to Presidents unwilling to take on large donors). Perhaps this is another way that the US is most susceptible in cyber war.

Conclusion

In closing, the book *Cyber War* does highlight genuine vulnerabilities: some existing since the creation of the Internet, and others brought about by middleware and other software designed to leverage the Internet's capabilities. Yet this image of a hacker unit bringing down vital systems continents away, comfortably, anonymously, solely through a computer terminal, is inconsistent with what has been deemed the first successful cyber attack in history: STUXNET.

While Trojans, backdoors and time-bombs have been variously used in early attempts to sabotage real vital systems, the success of STUXNET contrasts sharply, with its physical delivery via USB key and clear indications of intimate awareness of the target system. A lot of details of the target systems, systems presumably isolated from the Internet, were previously known to the cyber attacker, including the specific control numbers associated with the centrifuges, and the operating range values of those centrifuges. Genuine intelligence collection and operations were part of the STUXNET attack, in addition to the vulnerabilities in the Windows system and the SCADA, the Siemens industrial control software. Real leg-work was involved in this effort: it was not done from afar, and it was neither easy nor sterile.

In the following months after the publication of *Cyber War*, the U.S. response has been two-fold. First, the phrase "separate secure computer network" specifically for essential systems has been used time and again, suggesting that isolating a network

also helps to secure it (Shanker 2010). While this follows Clarke's assertions that a system on the Internet is essentially open to attack from anywhere on the globe, one wonders about the wisdom of creating a special insulated network composed entirely of systems absolutely vital to U.S. security. Such a network would invariably include more nodes than the SIPRNet or JWICS, if it were to include public sector "banking, aviation, and public utility systems" (Shanker 2010). The question would be whether USCYBERCOM could secure this larger civilian network any better than DoD's own classified networks. One must also consider the lesson of STUXNET: that intelligence operations, social engineering and the inside man, can get around isolation. More important, is the question regarding whether the NSA/USCYBERCOM commander is any more capable of exercising authority over telecommunications and electric utilities, and whether the President has to political will to back him.

Cyber-deterrence has been the second theme of U.S. cyber war preparations (Ignatius 2010, McConnell 2010). The Air Force specifically has lobbied for greater leeway in preparing such capabilities. And in the context of STUXNET, this does seem to make some sense. Remember that Iran had vowed a global retaliatory response to any strikes on its nuclear facilities. And yet after STUXNET's crippling attack (*DEBKAfile* 2010), nothing has happened. Apparently, the slow but sweeping infection of its SCADA didn't translate into the escalated response Iran had committed to earlier. A cyber attack might be an appropriate response in such instances, especially if one assumes unwillingness in the Executive office to escalate. This part of the story is still unfolding, and may change once cyber attacks become more common.

Appendix I: The Political Context

Richard Clarke didn't write his book in a vacuum, but did so in a specific context. In early 2010, the U.S. hadn't fully committed to a strategy for dealing with cyber war: in fact, there were many voices in opposition, convinced that the money would be better spent elsewhere.

Meanwhile, Russia and China appeared determined to develop and exploit cyber-attack capabilities: Russian usage had been typically tracked to private organizations primarily, including the mafia, although links to Russian intelligence have been made. Chinese usage was believed to have state military elements, with a dedicated cyber-corps (Libicki 2009). Both had repeatedly exercised cyber-warfare on nearby countries, including Estonia, Georgia, Kirgizstan, Taiwan, and South Korea. Both had also performed cyber attacks on the United States, particularly on defense systems and on defense companies. Lastly, France and Israel were also known to have actively pursued cyber-attack abilities (McAfee 2009).

The U.S. response could have been described as schizophrenic, occurring in fits and starts, before retreating to inaction. The mission has passed from one military command to another (White House 2009), and the military debated how useful it would be to assign resources to this, as compared to further investment to solidify positions of superiority, such as the dominance in areas where the US already has control: the command of the commons (Posen 2003).

Given the uncertainty behind the qualitative threat of cyber warfare, the state was left to generate conclusions with minimal evidence, relying on widely diverging opinions from think tanks, relevant government agencies, and industry (Yoran 2010). This was a concern especially since there were likely to be billions of dollars at stake for cyber-security spending.

As an example, House Resolution 4061: Cybersecurity Enhancement Act was long stalled in Senate (as of *Cyber War*'s publication), despite bipartisan sponsorship from Republican Olympia Snowe and Democrat John Rockefeller (Fulton 2010), along with other essentially domestic House Resolutions: H.R. 12: Paycheck Fairness Act, H.R. 2847: Jobs for Main Street Act, and H.R. 4194: Law Student Clinic Participation Act (*The Hill* 2010). Contrast the Cybersecurity Enhancement Act, with H.R. 730: Nuclear Forensics and Attribution Act and H.R. 2194: Iran Refined Petroleum Sanctions Act of 2009, each had been passed by both the House and Senate.

This impasse in Congress had its effects and had not gone unnoticed. On the civilian side, including the White House and the Department of Homeland Security, Melissa Hathaway, the Cybersecurity Czar who began work under President George W. Bush and had completed the Cyberspace Policy Review (White House 2009) under President Barack Obama, reportedly departed her post after being frustrated that the position had no powers, and that none of the recommendations made had been acted upon (Gorman 2009). Other high profile departures during this period included Rod Beckstrom and Amit Yoran, under frustrations over bureaucratic wrangling and government turf issues resulting from a failure to define organizational responsibilities.

The lack of responsiveness from Congress had also been a concern for the military side, to include the Department of Defense and the National Security Agency.

The nominee for the proposed double-hatted NSA/USCYBERCOM 4-star General position, then Lt. General Keith Alexander, wrote a 32 page response to the Senate Armed Services Committee detailing the areas where legal restrictions were out of step with the evolving cyber threat (Shanker 2010). Again, as of *Cyber War*'s publication, USCYBERCOM had yet to fully stand up, and Lt. General Alexander remained a 3-star general.

Also, the various branches of the armed services were jockeying for lead roles in cyber warfare, as extensions of their existing missions in information warfare. Causes ranged from funding predominance for the Army and Marines in the present wars, to role expansion-seeking of the younger Air Force, to the usual money chase exhibited by any federal organization. This was unsurprising given the vacuum of legal guidance on which agency should play a lead role in handling the emerging threat. At the same time, the question of why the military should even be involved had been raised, considering the reality that the military capabilities were very limited in handling or responding to cyber threats, being practically limited to high-powered RF injections (Fulghum 2010).

Then there was the National Security Agency, which at first downplayed its role in cyber warfare (Zetter 2009); something it did rather than simply remaining silent on the issue, which seems completely baffling. Yet its obvious positioning to handle the task led Rod Beckstrom to resign as the Department of Homeland Security's Director of the National Cybersecurity Center, citing his disagreement with that agency's participation. In the end, the obvious solution that could be implemented, a sub-unified command under USSTRATCOM headed by the NSA director would be selected.

However, even with clear guidance available on which agencies will be tackling the specific issue, government organizations were still unable to coordinate with one

another. In early 2010, the Department of Defense dismantled a CIA anti-terror website in Saudi Arabia via cyber attack, citing that it also functioned as a terrorist networking site. This infuriated the CIA and embarrassed the agency in front of several Saudi princes with whom it was collaborating (Nakashima 2010). It was clear that the bureaucracy needed coordination and specific direction regarding the division of labor. As stated above, the consolidation of cyber warfare under USCYBERCOM had yet to be fulfilled (and the memory of where to even locate such a force is likely still fresh in the minds of certain legislators). And the then-imminent anointing of the NSA/USCYBERCOM single commander was stalled in Congress.

Appendix II: Timeline

To provide a common knowledge base from which to argue, a brief and selected history of relevant events follows. It is by no means comprehensive or exhaustive, but a little information might provide insight into the precise nature of the threat (adapted from multiple sources, mainly Libicki 2009; McAfee 2009; White House 2009). This is a broad brush overview; specifics will be discussed in the relevant sections. Note the increasing complexity and politicization of attacks over time. Also note how there is a clear development of cyber attacks towards what is observed today.

(D)ARPA (1958): In response to the USSR's launch of Sputnik, the (Defense) Advanced Research Projects Agency is formed to ensure American technological parity at minimum, with an objective of technological dominance.

ARPANET (1969): First nodes of packet-based precursor to modern day Internet are connected in California. The first international connection made in 1978, eventually consolidating on TCP/IPv4 packet specification (1980s).

PERSONAL COMPUTING (1970s): Development of the modem, and "micro" computers designed for home use, as opposed to server-terminal architecture. Concurrently, initial forays into device-hacking begin, including the famous 2600 Hz method of fooling telephone exchanges.

MITNICK, KEVIN (1980s): Once the most wanted hacker in America, alleged to have gained remote PC access to NORAD servers. Known to have cloned cellular phone numbers and stolen private enterprise software.

WORLD WIDE WEB (1990s): Interface adopted, followed by a period of explosive growth of the internet as most private nets connect into the vast decentralized network. ICANN manages the IP address assignment and Domain Name System, while IETF handles the technical specification of communication standards and protocols, such as IPv4 and IPv6. WWWC advances the HTML specification.

VBSCRIPT (1990s): As Microsoft Windows, Internet Explorer and Outlook dominate home computing, Visual Basic Scripts are frequently used to create viruses transmitted via email, often merely being variations of one another. (To help the consumer, Microsoft automated running such scripts whenever one is received.) This culminates in the MELISSA virus and the ILOVEYOU virus, both known to have slowed internet traffic.

OPERATION ALLIED FORCE (1999): Bombing of Serbian forces in Kosovo, the U.S. is alleged to have broken into Serbian air warning systems to confuse Serbian air defenses, and thus permit U.S. air forces greater freedom of action over Kosovo. Meanwhile Serbian attempts to affect American systems are ineffective.

MOONLIGHT MAZE (1999): Alleged but not confirmed attacks on U.S. Department of Defense systems and related defense-related corporations. Believed to have originated from Russia.

NIMDA (2001): Internet worm notable for its multiple infection vectors. Known to have slowed internet traffic down.

SQL SLAMMER (2003): Worm exploiting a buffer overflow vulnerability in Microsoft's implementation of the SQL server. Known to have slowed internet traffic down.

OPERATION IRAQI FREEDOM (2003): U.S. considers but ultimately declines to perform a cyber attack on Iraqi banking and economic institutions in the run-up to invasion.

TITAN RAIN (2003): Espionage attacks on U.S. Department of Defense systems and related defense-oriented corporations. Believed to have originated from China.

ESTONIA (2007): After moving a Soviet War Memorial out of the town center, this small republic endures an attack on its government and private networks, allegedly originating from Russia. Vital services in this highly net-oriented economy are disrupted.

ZEUS BOTNET (2007): Trojan with keystroke logger designed to steal banking information, remains active with new versions, having infection rates still in the millions.

GEORGIA (2008): During the South Ossetia war, Georgian computer systems are compromised. Government websites are defaced, and internet services are disrupted. Believed to have originated from Russia.

CONFICKER (2008): Windows worm, still affecting thousands of machines comprising a massive BotNet. Notable for its advanced methods of obfuscation, and being able to be updated post-initial infection, still in the millions. Believed to have originated from Ukraine.

KIRGHIZSTAN (2009): Major distributed denial of services (DDoS) attack, allegedly originating from Russia, on this central Asian republic, disrupts the majority of all internet traffic, especially to the West.

U.S. POWER GRID (2009): U.S. intelligence agencies identify an attack on the U.S. power grid and other civil infrastructure networks, designed to remotely disrupt services at some point in the future. The attacks are alleged to have come from Russia and China.

GHOSTNET (2009): Chinese operation relying on a Trojan virus to gain control of Windows based machines, targeting computers systems of countries and organizations hosting or supporting the Dalai Lama.

JULY BOTNET ATTACKS (2009): Latent BotNet, or group of compromised computers, used to perform DDoS attacks on commerce sites in the U.S. and South Korea. North Korea was believed to be involved, although likely had outside help.

OPERATION AURORA (2010): Google revealed that attacks occurred on their information systems and on the systems of other major U.S. corporations (including defense oriented ones). The sophisticated attack on multiple U.S. companies was accomplished using obscure vulnerabilities, conducted using intermediary servers in the U.S. and Taiwan. China is believed to be the origin.

USCYBERCOM (2010): Centralized military hub awaits complete stand-up. Military mission has passed from provisional organization to provisional organization for over a decade. From JTF-CND, to SPACECOM, to USCYBERCOM, to USCYBERCOM under STRATCOM.

STUXNET (2010): See Conclusion above.

A casual reading of this list of events should point to a clear progression. On one hand, the sophistication of the attacks has grown, from the old VBScripts, phishing, and social engineering, to massive and update-capable botnets, concealed attack methods, and continual discovery of obfuscated vulnerabilities (while still using phishing and social

engineering). On the other hand, the attacks have grown increasingly politicized, either in concert or as a prelude to both civil and military intervention, as envisioned by Qiao and Wang (1999).

And these trends are likely to continue. With each generation of software development, backwards compatibility hooks and libraries must be continually added, resulting in a multi-layered mess; in every machine, software still sits atop heaps of unmaintainable legacy code, even in clean new installs. And as seen in the history, norms of behavior have developed such that it has become commonplace for states to employ programmers to exploit these weaknesses for political purposes.

Yet why were these patterns missed, and why do many doubts remain both in private and public positions? Consider the 9/11 Commission Report's explanation on why the continental United States was attacked in 2001 without being cognizant of the warning signs: “Imagination is not a gift usually associated with bureaucracies” (Kean 2004).

Bibliography

Arquilla, John, and David Ronfeldt. (2001) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND Corporation.

Banks, Darwyn O. (2001) "Information War Crimes: Mitnick Meets Milosevic." Research paper for Air Command and Staff College.

Blunden, Bill. (2010) "Manufactured Consent and Cyberwar." *Below Gotham Labs*. Conference Proceedings from Lockdown 2010, University of Wisconsin-Madison.

Bradley, Tom. (2010 "GSM Phone Hack FAQ: What You Should Know." *PCWorld*. http://www.pcworld.com/businesscenter/article/202317/gsm_phone_hack_faq_what_you_should_know.html (Accessed 5 August 2010).

Carden, Michael J. (2010) "Cyber Task Force Passes Mission to Cyber Command." *American Forces Press Service*. http://www.globalsecurity.org/security/library/news/2010/09/sec-100907-afps01.htm (Accessed 7 September 2010).

Carr, Jeffrey. (2010) "The War That We Don't Recognize Is The War We Lose." *Greylogic*. http://greylogic.us/2010/07/12/the-war-that-we-dont-recognize-is-the-war-we-lose (Accessed 12 July 2010).

Cavelty, Myriam D. (2007) "Cyber-Terror--Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology and Politics* 4 1 (December): 19-36.

Clarke, Richard A. (2010) *Cyber War: The Next Threat to National Security and What to do About It*. Harper Collins Publishers: New York.

Clayton, Mark. (2010) "Son of Stuxnet? Variants of the cyberweapon likely, senators told." *The Christian Science Monitor*. http://www.csmonitor.com/USA/2010/1117/Son-of-Stuxnet-Variants-of-the-cyberweapon-likely-senators-told (Accessed 17 November 2010).

_____, Mark. (2010) "How Stuxnet cyber weapon targeted Iran nuclear plant." *The Christian Science Monitor*. http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant (Accessed 19 November 2010).

Collins, Hilton. (2010) “Advanced Cyber-Attacks on the Rise in 2010, Report Says.” *Government Technology*. http://www.govtech.com/security/Advanced-Cyber-Attacks-on-the-Rise-in.html (Accessed 21 July 2010).

Conway, Maura. (2007) “Cyber-Terrorism: Hype and Reality.” In *Information Warfare: Separating Hype from Reality*, ed. E. Leigh Armistead. Dulles: Potomac Books.

DEBKAfile staff. (2010) “An alarmed Iran asks for outside help to stop rampaging Stuxnet malworm.” *DEBKAfile*. http://www.debka.com/article/9050 (Accessed 29 September 2010).

Dhanjani, Nitesh, Billy Rios and Brett Hardin. (2009) *Hacking: The Next Generation*. Sebastopol, CA: O’Reilly Media.

Eriksson, Johan and Giampiero Giacomello. (2006) “The Information Revolution, Security, and International Relations: (IR)relevant Theory?” *International Political Science Review* 27 3 (July): 221-244.

The Economist Staff. (2010) “Cyberwar.” *The Economist*. http://www.economist.com/node/16481504?story_id=16481504 (Accessed 1 July 2010).

Falliere, Nicholas, Liam O. Murchu, and Eric Chien. (2010) “W32.Stuxnet.Dossier.” Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (Accessed 28 October 2010).

Fisher, Dennis. (2010) “NSA Director Says U.S. Has Duty to Secure the Internet.” *threatpost*. http://threatpost.com/en_us/blogs/nsa-director-says-us-has-duty-secure-internet-090710 (Accessed 7 September 2010).

Flynn, Stephen E. (2002) “America the Vulnerable.” Foreign Affairs 81(1): 60-74.

Fulghum, David A. (2010) “US Cyber-Combat needs Rules.” *Aviation Week and Space Technology*. http://www.military.com/features/0,15240,212587,00.html (Accessed 23 March 2010).

Fulton, Scott M. (2009) “Obama's cybersecurity chief resigns, signals disarray.” *Betanews*. http://www.betanews.com/article/Obamas-cybersecurity-chief-resigns-signals-disarray/1249407324 (Accessed August 4 2009).

_____, Scott M. (2010) “Federal cybersecurity authority awaits break in Senate logjam.” *Betanews*. http://www.betanews.com/article/Federal-cybersecurity-authority-awaits-break-in-Senate-logjam/1266943835 (Accessed February 23 2010).

Geist, Michael. (2010) “Geist: Lawful access regulation would reshape Canada’s Internet.” *The Star*. http://www.thestar.com/news/sciencetech/technology/lawbytes/article/889359--geist-

lawful-access-legislation-would-reshape-canada-s-internet (Accessed 15 November 2010).

Ghosh, Bobby. (2009) “How Vulnerable is the Power Grid.” *Time*. http://www.time.com/time/nation/article/0,8599,1891562,00.html (Accessed 16 April 2009).

Gjelten, Tom. (2010) “Cyberwarrior Shortage Threatens U.S. Security.” *NPR*. http://www.npr.org/templates/story/story.php?storyId=128574055 (Accessed 19 July 2010).

Glenny, Misha. (2010) “Cyber War.” *Financial Times*. http://www.ft.com/cms/s/2/6ba1923e-66bc-11df-aeb1-00144feab49a.html (Accessed 24 May 2010).

Gorman, Siobhan. (2009) “Security Cyber Czar Steps Down.” *The Wall Street Journal*. http://online.wsj.com/article/SB124932480886002237.html (Accessed 5 April 2009).

_____, Siobhan. (2009) “Electricity Grid in U.S. Penetrated by Spies.” *The Wall Street Journal*. http://online.wsj.com/article/SB123914805204099085.html (Accessed 8 April 2009).

_____, Siobhan. (2010) “Broad New Hacking Attack Detected.” *The Wall Street Journal*. http://online.wsj.com/article/SB10001424052748704398804575071103834150536.html (Accessed 18 February 2010).

_____, Siobhan. (2010) “U.S. Plans Cyber Shield for Utilities, Companies.” *The Wall Street Journal*. http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html (Accessed 8 July 2010).

Hansen, Lene and Helen Nissenbaum. (2009) “Digital Disaster, Cyber Security, and the Copenhagen School.” International Studies Quarterly 53 4 (December): 1155-1175.

Hart, Gary and Warren B. Rudman. (2002) *America--Still Unprepared, Still in Danger*. New York: Council on Foreign Relations.

Hayes, Richard E., and Gary Wheatley. (1996) “Information Warfare and Deterrence.” *Strategic Forum* 87 (October): 1-6.

Hersh, Seymour M. (2010) “The Online Threat.” *The New Yorker*. http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh (Accessed 4 November 2010).

Hildreth, Steven A. (2001) “Cyberwarfare.” Congressional Research Service Report for Congress, The Library of Congress.

The Hill Staff. (2010) “The 290 Bills That Have Been Passed by the House & Not Yet Acted Upon By the Senate, as of 2/12/10.” *The Hill*. http://thehill.com/homenews/senate/83057-290-bills (Accessed February 23, 2010).

Ignatius, David. (2010) “Pentagon’s cybersecurity plans have a cold war chill.” *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/25/AR2010082505962.html (Accessed 26 August 2010).

Kakutani, Michiko. (2010) “The Attack Coming From Bytes, Not Bombs.” *The New York Times*. http://www.nytimes.com/2010/04/27/books/27book.html (Accessed 13 July 2010).

Kean, Thomas H., et al. (2004) *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Report to Congress.

LaFraniere, Sharon and Jonathan Ansfield. “China Alarmed by Security Threat From Internet” *The New York Times*. http://www.nytimes.com/2010/02/12/world/asia/12cyberchina.html (11 February 2010).

Leiber, Kier. (2005) *War and the Engineers: The Primacy of Politics over Technology*. Ithaca and London: Cornell University Press.

Lewis, James A. (2002) “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.” Center for Strategic & International Studies.

_____, James A. (2007) “Cyber Attacks Explained.” Center for Strategic & International Studies.

_____, James A. (2008) “Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency.” Center for Strategic & International Studies.

Libicki, Martin C. (1995) *What is Information Warfare?* Washington: National Defense University.

_____, Martin C. (2007) *Conquest in Cyberspace.* Cambridge: Cambridge University Press.

_____, Martin C. (2009) *Cyberdeterrence and Cyberwar.* Santa Monica: RAND Corporation.

Markoff, John, David E. Sanger, and Thom Shanker. (2010). “In Digital Combat, U.S. No Easy Deterrent.” *The New York Times*. http://www.nytimes.com/2010/01/26/world/26cyber.html (Accessed 25 January 2010).

Markoff, John and David Barboza. (2010) “Chinese Academics' Paper Sets Off Alarms in U.S.” *The New York Times*. http://www.nytimes.com/2010/03/21/world/asia/21grid.html (Accessed 20 March 2010).

_____, John and David Barboza. (2010) “Researchers Trace Data Theft Intruders to China.” *The New York Times*. http://www.nytimes.com/2010/04/06/science/06cyber.html (Accessed 6 April 2010).

McAfee Associates. (2009). *Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare*. http://resources.mcafee.com/content/NACriminologyReport2009NF (Accessed 17 November 2009).

_____. (2010). *McAfee Threats Report: Third Quarter 2010*. http://www.mcafee.com/us/local_content/reports/q32010_threats_report_en.pdf (Accessed 15 November 2010).

McConnell, Michael. (2010) “Mike McConnell on how to win the cyber-war we're losing.” *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (Accessed February 28 2010).

McCullagh, Declan. (2010) “Senators propose granting president emergency Internet power.” *CNET*. http://news.cnet.com/8301-13578_3-20007418-38.html (Accessed 10 June 2010).

_____, Declan. (2010) “Liebermann defends emergency Net authority plan.” *CNET*. http://news.cnet.com/8301-13578_3-20007851-38.html (Accessed 15 June 2010).

_____, Declan. (2010) “U.S. military cyberwar: What’s off-limits?” *CNET*. http://news.cnet.com/8301-31921_3-20012121-281.html (Accessed 30 July 2010).

Mills, Elinor. (2010) “Details of the first-ever control system malware (FAQ).” *CNET*. http://news.cnet.com/8301-27080_3-20011159-245.html (Accessed 21 July 2010).

Morozov, Evgeny. (2009) “10 easy steps to writing the scariest cyberwarfare article ever.” *Foreignpolicy.com*. http://neteffect.foreignpolicy.com/posts/2009/04/11/writing_the_scariest_article_about_cyberwarfare_in_10_easy_steps (Accessed 14 April 2009).

_____, Evgeny. (2010) “Battling the Cyber Warmongers.” *The Wall Street Journal*. http://online.wsj.com/article/SB10001424052748704370704575228653351323986.html (Accessed 8 May 2010).

Nakashima, Ellen. (2010) “Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies.” *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html (Accessed 19 March 2010).

_____, Ellen. (2010) “Defense official discloses cyberattack.” *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.html (Accessed 24 September 2010).

Nye, Joseph S. (2008) “Cyber Insecurity.” *Daily News Egypt*, December 14.

Posen, Barry. (2003) “Command of the Commons: The Military Foundations of U.S. Hegemony.” *International Security* 28 1 (Summer): 5-46.

Qiao Liang and Wang Xiangsui. (1999) *Unrestricted Warfare*. trans. Foreign Broadcast Information Service. Beijing: PLA Literature and Arts Publishing House.

Rattray, Greg. (2001) *Strategic Warfare in Cyberspace*. Cambridge: The MIT Press.

Reynolds, Glenn H. (2010) “Tinker, Tailor, Soldier, Hacker.” *The Wall Street Journal*. http://online.wsj.com/article/SB10001424052748704671904575193942114368842.html (Accessed 26 April 2010).

Shanker, Thom. (2010) “Cyber Nominee Sees Gaps in Law.” *The New York Times*. http://www.nytimes.com/2010/04/15/world/15military.html (Accessed 14 April 2010).

_____, Thom. (2010) “Cyberwar Chief Calls for Secure Computer Network.” *The New York Times*. http://www.nytimes.com/2010/09/24/us/24cyber.html (Accessed 24 September 2010).

Stanton, John. 2000. “Rules of Cyber War Baffle U. S. Government Agencies.” *National Defense* 84 (February): 29-30.

Stein, Jeff. (2010) “Book review: ‘Cyber War’ by Richard Clarke.” *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2010/05/21/AR2010052101860.html (Accessed 27 May 2010).

Vijayan, Jaikumar. (2010) “New malware targets utility systems.” *Computerworld*. http://www.computerworld.com/s/article/350976/New_Malware_Targets_Utility_Control_Systems (Accessed 12 August 2010).

Wexler, Joanie. (2010) “WPA2 vulnerability found.” *NetworkWorld*. http://www.networkworld.com/newsletters/wireless/2010/072610wireless1.html (Accessed 26 July 2010).

The White House. (2009) “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.” http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (Accessed 5 June 2009).

_____. (2010) “The Comprehensive National Cybersecurity Initiative.” http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (Accessed March 7 2010).

Yoran, Amit. (2010) “Cyberwar Or Not Cyberwar: And Why That Is The Question.” *Forbes.com.* http://blogs.forbes.com/firewall/2010/03/25/cyberwar-or-not-cyberwar-and-why-that-is-the-question (Accessed 25 March 2010).

Zetter, Kim. (2008) “Revealed: The Internet’s Biggest Security Hole.” *Wired.* http://www.wired.com/threatlevel/2008/08/revealed-the-in/ (Accessed October 12 2010).

_____, Kim. (2009) “NSA Chief: ‘We Do Not Want to Run Cyber Security.’” *Wired*. http://www.wired.com/threatlevel/2009/04/post-2 (Accessed 21 April 2009).

_____, Kim. (2009) “Obama Cybersecurity Report Addresses Critical Infrastructure and Privacy Issues.” *Wired*. http://www.wired.com/threatlevel/2009/05/5638 (Accessed 29 May 2009).

_____, Kim. (2010) “Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target.” *Wired*. http://www.wired.com/threatlevel/2010/09/stuxnet (Accessed 23 September 2010).

VITA

Jonathan Iming Lee was born in Palo Alto, California. After attending Horace Greeley High School, Chappaqua, New York, he entered Tufts University in Medford, Massachusetts. During the summers he worked for the physics department there. He received a Bachelor of Science from Tufts University in May, 2001. During the following years he was commissioned and served as a Line Officer in the United States Air Force. In September 2006 he entered the Graduate School at the University of Texas at Austin.

Contact information: jil229@mail.utexas.edu

This report was typed by the author.