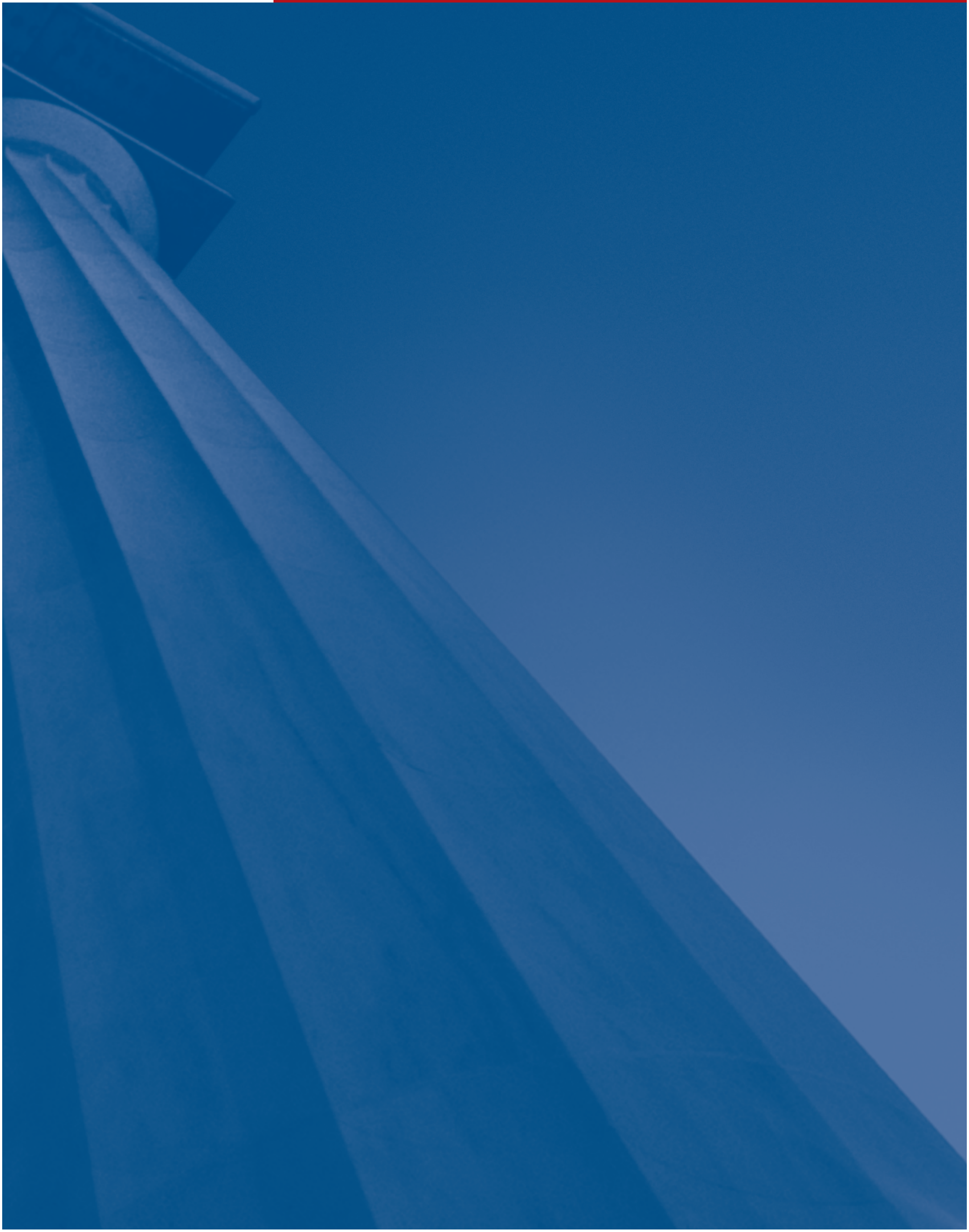
CHAPTER III:
SEPARATING THREAT FROM THE HYPE: WHAT WASHINGTON NEEDS TO KNOW ABOUT CYBER SECURITY

By Gary McGraw and Nathaniel Fick

JUNE 2011

America's Cyber Future

Security and Prosperity in the Information Age



SEPARATING THREAT FROM THE HYPE: WHAT WASHINGTON NEEDS TO KNOW ABOUT CYBER SECURITY

By Gary McGraw and Nathaniel Fick

Washington has become transfixed by cyber security and with good reason. Cyber threats cost Americans billions of dollars each year and put U.S. troops at risk.[1] Yet, too much of the discussion about cyber security is ill informed, and even sophisticated policymakers struggle to sort hype from reality. As a result, Washington focuses on many of the wrong things. Offense overshadows defense. National security concerns dominate the discussion even though most costs of insecurity are borne by civilians. Meanwhile, effective but technical measures like security engineering and building secure software are overlooked.

The conceptual conflation of cyber war, cyber espionage and cyber crime into a monolithic and dangerous "cyber menace" perpetuates fear, uncertainty and doubt. This has made the already gaping policy vacuum on cyber security more obvious than ever before. But as Washington grapples with the challenge of cyber security, the risks – which range from failing to act, to acting poorly to overreacting – are real and have far-ranging consequences.

When it comes to cyber security, it is hard even for experts to understand what is real and what is a cyber chimera. How much of what we are hearing about cyber war is driven by hype? How much of it is something that we need to worry about, and who should do the worrying? More to the point, if the hype and fear engines ran out of fuel for a day, leaving only even-handed and well-reasoned analysis, how would we describe the current situation and begin to create an approach for improvement? Our aim in this chapter is to help policymakers find their way through the fog and set guidelines to protect the best of the Internet and cyberspace, both from those who seek to harm it, and from those who seek to protect it but risk doing more harm than good.

Cyber Hype and Cyber Reality

Any discussion of cyber security must begin by separating hype from reality. It is true that cyber war, cyber espionage and cyber crime all share the same root cause – dependence on insecure cyber systems. The bad news about U.S. cyber dependency is that cyber war appears to be dominating the conversation among policymakers even though cyber crime is a much larger and more pervasive problem. When pundits and policymakers focus only on the dangers of cyber war, the most pressing threats emanating from cyber espionage and cyber crime are relegated to the background.

WHAT IS CYBER WAR?

Whether online, on television or in print, hyperbolic discussion of cyber war has become widespread. The most hyped of these "cyber war" stories are worth reviewing:

- Hyped Story #1 – In 2007, a number of distributed denial-of-service (DDoS) attacks, in which many coordinated computers overwhelm a target computer with messages and thereby block legitimate traffic, were directed against Estonia. This happened during a political dust-up with Russia over the removal of a statue. While the complexity of modern conflict makes it difficult to draw perfect distinctions, the DDoS attack against Estonia had no warlike impact. Most importantly, the technical sophistication of the attacks was very low. In 2009, similar cyber attacks targeted the Republic of Georgia during the Russian armed invasion. However, from a technical standpoint, attacks like these would fail utterly if launched against popular U.S. e-commerce websites such as Amazon or Google, possibly to the point of not even being noticed.[2]
- Hyped Story #2 – In 2009, CBS aired a segment on its show *60 Minutes* that attributed several blackouts in Brazil to unidentified cyber attackers. Brazil's top cyber security officer denied the allegations.[3] A few days after the show aired, a major blackout in Brazil prompted renewed speculation of cyber attacks. The subsequent discovery of some very minor implementation bugs involving databases in the power company's website provided feeble evidence in support of the claim.[4] Nonetheless, speculation about a cyber attack surged. Ultimately, an investigation revealed the blackout was the much more pedestrian result of a combination of operational and procedural failures from one electric power supplier company.[5]
- Hyped Story #3 – In 2010, a mistake made when managing one of the protocols at the heart of the Internet called Border Gateway Protocol (BGP) was incorrectly characterized as a malicious "hijacking" of 15 percent of U.S.-based Internet traffic by Chinese attackers.[6] The mistake led to a temporary and short-lived diversion of traffic on some segments of the Internet through servers in China. Much of the spin characterized the mistake, which is unfortunately very easy to make due to the poor design of BGP, as an intentional and malicious act. Though the actual traffic numbers in question were inflated, even members of the U.S. Congress appear to have regarded this incident as a deliberately orchestrated cyber attack.[7]

It is a bad idea to intermingle hyped stories such as these with more severe attacks. Doing so obscures understanding of the seriousness of cyber warfare and its implications. Though computer geeks and policy wonks must work together to solve cyber security problems, continuing to use a loose definition of cyber war risks alienating experts who see through computer security jargon and hype. Distributed denial-of-service attacks with no physical impact should not be used as an example of cyber war. Doing so will only widen the chasm between computer security specialists and Washington decision makers.[8]

Compounding the misinformation spread by these kinds of stories is the lack of a clear definition of cyber war. Definitions vary widely. The "war" part is relatively straightforward: Violent conflict between groups for political, economic or philosophical reasons. The less straightforward part is determining whether an action with no real world impact constitutes cyber war. For example, is simply taking down a website or infecting a computer with a malicious virus an act of cyber war? Although sometimes framed as such, this definition seems far too sweeping.

When pundits and policymakers focus only on the dangers of cyber war, the most pressing threats emanating from cyber espionage and cyber crime are relegated to the background.

Cyber war requires a consequential impact in the physical world, or what military experts call a "kinetic" (or physical) impact. Infecting an adversary's command and control system with malicious software yielding the attacker complete control, thereby allowing the attacker to command the adversary's Predator drones to shoot at the wrong targets would, for example, count as an act of cyber war. In the end, war is the application of force to achieve a desired end. Or, as Prussian military theorist Carl von Clausewitz famously put it, war is the continuation of politics by other means. To qualify as cyber war, the means may be virtual, but the impact should be real.

To be sure, some cyber attacks do transcend the confines of cyberspace and qualify as cyber war.

In their recent book, *Cyber War*, Richard Clarke and Robert Knake include a number of case studies that illustrate the notion of kinetic impact.[9] Perhaps the most interesting example involves Israeli cyber war maneuvers during the bombing of a suspected Syrian nuclear facility in 2007.[10] Syria's formidable air defense system could not track inbound Israeli fighter jets because it was taken over by Israeli cyber warriors who incapacitated or otherwise blinded it before the raid. This meets the definition of cyber war; the tie to a kinetic impact is clear – a completely destroyed Syrian facility.

There are a number of additional examples of real cyber attacks going back decades that are worth mentioning. In 1982, Canadian computer code, modified by the CIA before it was stolen by the Soviets, caused a Soviet gas pipeline to explode. Last year and perhaps earlier, the Stuxnet worm was used to attack uranium enrichment facilities in Iran. While analysis of Stuxnet continues to this day, it appears to be a real offensive cyber weapon with a clear kinetic impact, namely, non-functioning centrifuges.[11] Stuxnet is a fascinating study in the future of malicious software or "malware." Not only did its delivery vehicle reveal at least four previously unknown exploits in Microsoft software, its payload clearly demonstrated that systems of the sort that control power plants and safety-critical industrial processes are rife with vulnerabilities.[12]

Another real and serious instance of a cyber attack occurred in 2008, when a USB drive in the Middle East was used to infect U.S. Department of Defense command and control systems, prompting Deputy Secretary of Defense William Lynn to write in *Foreign Affairs*, "This previously classified incident was the most significant breach of U.S. military computers ever, and it served as an important wake-up call."[13] However, the impact of this attack appears to have remained limited to cyberspace.

War has both defensive and offensive aspects, and understanding this fundamental dynamic is central to understanding cyber war. Overconcentrating on offense can be very dangerous and destabilizing as it encourages actors to attack first and ferociously, before an adversary can since no effective defense is available. On the other hand, when defenses are equal or even superior to offensive forces, actors have less incentive to strike first because the expected advantages of doing so are far less. The United States is supposedly very good at cyber offense today, but from a cyber defense perspective it lives in the same glass houses as everyone else. The root of the problem is that the systems we depend on – the lifeblood of the modern world – are not built to be secure.

This notion of offense and defense in cyber security is worth teasing out now and returning to later. In our view, *offense* involves exploiting systems, penetrating systems with cyber attacks and generally leveraging broken software to compromise entire systems and systems of systems.[14] On the other hand, *defense* means building secure software, designing and engineering systems to be secure in the first place and creating incentives and rewards for systems that are built to be secure.[15]

Unlike physical reality, cyberspace has a completely different makeup that affects the mix of offense and defense. It is impossible to "take and hold" cyberspace, to invoke a term traditionally used in military operations. Cyberspace more closely resembles the naval or space domains where powerful countries are able to monitor, patrol, exert influence and deter aggression, but they do not exercise control in the way it is traditionally conceived of during ground conflicts. Cyber sharpshooters cannot control a section of cyberspace and should not be asked to do so.

Indeed, cyberspace is a dynamic system in constant motion where clocks run at superhuman tempo close to the speed of light. Time and space are different in cyberspace. There is no "there" there, and humans are intolerably slow.

There is also no isolated battlefield on the Internet. In the case of cyber war, the battlefield will, by necessity, involve civilian systems of every stripe.

In the final analysis, the threat of cyber war is real but overstated. Even acts amounting to cyber war have thus far never led to military conflict in the real world.

WHAT IS CYBER ESPIONAGE?

Cyber espionage is another prominent cyber security problem that captivates the imagination. Cyber espionage is much more common than cyber war. The highly distributed, massively interconnected nature of modern information systems makes keeping secrets difficult. When almost one million U.S. citizens have security clearances and information system managers are told that "connecting the dots" should be their top method for stopping terrorism, it should come as little surprise that classified information often leaks. It is easier than ever before to transfer, store and hide information. A pen drive the size of a little finger can store more information than the super computers of a decade ago.

WikiLeaks is not an anomaly. That is, the WikiLeaks commotion that grabbed headlines is not just the result of a lone information terrorist; it also resulted from flawed policy on the part of the U.S. government. Other than perhaps some minor deterrent effects, prosecuting the leadership of WikiLeaks does absolutely nothing to fix the root cause of cyber espionage. The better solution is reasonable information system policy and proper technology enforcement, including the proper engineering of systems so that they are secure.

Civilian and corporate espionage is also a factor in cyber security. Look no further than the so-called "Operation Aurora" attacks by Chinese hackers against technology companies such as Google.

Laissez-faire information stances combined with overly lax cyber security policy means that cyber espionage and intellectual property infringement are easier to pull off than they should be. The target environment is ripe for the picking, and the Aurora episode, in which the Chinese spirited away vast quantities of intellectual property, is something to expect more of and to prepare for now.

> *Why did Willie Sutton, the notorious Depression-era gangster, rob banks? As he famously (and perhaps apocryphally) put it, "That's where the money is." Criminals flock to the Internet for the same reason.*

Unfortunately, the theft of intellectual property and company secrets appears not to be alarming enough for some who hype cyber threats. Some of the most shrill hypemongers misconstrue espionage as war, in effect arguing, "We may call it espionage, but it's really warfare because they're planting logic bombs," while offering little actual evidence of such activity.

WHY NOT CYBER CRIME?

Among the three major cyber security concerns in the public eye, cyber crime is far more pervasive than cyber war and cyber espionage, yet is the least commonly discussed. By every measure and according to every public report, cyber crime is growing and already commonplace. Indeed, 285 million digital records were breached in 2008 alone, with 79 percent of those breaches resulting from attacks against programs that run on the Web through Internet browsers.[16] Cyber crime and data loss are estimated to cost the global economy at least 1 trillion dollars each year.[17] Perhaps because it is so common, cyber crime is easy to overlook. The fact is, as consumers flock to the Internet, so do criminals. Why did Willie Sutton, the notorious Depression-era gangster, rob banks? As he famously (and perhaps apocryphally) put it, "That's where the money is." Criminals flock to the Internet for the same reason.

It is abundantly clear to most computer security professionals that cyber crime is a major and very real concern that needs to be addressed. Cyber crime is orders of magnitude more prevalent than cyber war and cyber espionage.

Interestingly, building systems properly from a security perspective will address the cyber crime problem just as well as it will address cyber espionage and cyber war. We can kill all three birds with one stone.

Washington's Distorted Focus

Because of the hype surrounding cyber war, Washington's focus has become distorted. Developing offensive capabilities has taken precedence over strengthening cyber defenses. Meanwhile, concern about military vulnerabilities and the concentration of resources there has led the national security establishment to dominate cyber security policy.

CYBER DEFENSES IGNORED

For years, computer security professionals have been attempting to protect systems riddled with security defects from potential attackers by placing a barrier between the broken stuff and the bad people. That is what firewalls are all about. But this endeavor has failed. Instead of continuing to sink resources into this flawed approach, we need to fix the broken stuff so that attacking it successfully takes far more resources and skill than is currently the case.[18] Concentrating on the improving offensive cyber capabilities simply will not alleviate dependence on vulnerable cyber systems. Concentrating on improving defense through proper engineering is a much better route.

The United States has reportedly developed formidable cyber offenses. Yet America's cyber defenses remain weak. What passes for cyber defense today – actively watching for intrusions, blocking attacks with network technologies such as firewalls, law enforcement activities and protecting against malicious software with anti-virus technology – is little more than a cardboard shield.

> *It is much catchier to talk about cyber offense and its impacts than to focus on defense and building things right in the first place.*

What we identify as "the NASCAR effect" applies, causing shortsighted pundits to focus on offense, which is sexy, to the detriment of defense, which is engineering.[19] Nobody watches NASCAR racing to see cars driving around in circles. They watch for the crashes. People prefer to see, film and talk about crashes more than building safer cars. There is a reason why there is no Volvo car safety channel on television even when there are so many NASCAR channels.

This same phenomenon happens in cyber security. In our experience, people would rather talk about cyber war, software exploit, digital catastrophe and shadowy cyber warriors than talk about security engineering, proper coding, protecting supply chains and building security in.[20] It is much catchier to talk about cyber offense and its impacts than to focus on defense and building things right in the first place.

Simply put, America has neglected its cyber defenses because strengthening them is a painstaking and unglamorous task. Because of the NASCAR effect, emphasizing cyber offense attracts more attention and funding than a more prosaic focus on defense and building security into software at the outset. Ultimately, a balanced approach to cyber security requires offense and defense in more equal measures.

NATIONAL SECURITY DOMINATES CYBER SECURITY

Thus far, the national security establishment has taken the lead on cyber security. The Pentagon established U.S. Cyber Command in 2009 to defend military networks against hacker attacks and consolidate cyber capabilities and personnel under a single authority.[21] To the extent that Cyber Command focuses on defense, so far it has been more reactive than proactive, concentrating on how to protect networks that are already vulnerable and seeking out malware already propagating on the network. Cyber Command also appears to be developing an impressive array of offensive capabilities, though these remain highly classified and the subject of media speculation.

Meanwhile, the civilian networks that account for at least 90 percent of America's cyber exposure go largely unappreciated. No agency inside the U.S. government has line responsibility for securing them. Insofar as civilian networks receive any attention from policymakers, the focus, once again, is on reacting rather than on building in security from the beginning.

Discussions outside government tend to underscore that cyber security is chiefly the purview of the national security establishment. The media emphasizes the U.S. defense industry, the U.S. intelligence community and the burgeoning cyber security industry. What the civilian high-technology sector and civilian agencies within the U.S. government can contribute to cyber security goes overlooked.

The real and perceived dominance of the U.S. national security establishment in setting cyber security policy is problematic in several respects. First, cyber security is neither solely nor primarily a military problem but rather a confluence of economic, cultural, diplomatic and social issues. Ignoring these dimensions and devoting singular focus to the military aspects of cyber security – the inevitable result of putting national security agencies in the lead – will result in a flawed approach.

Second, cyber security is a global problem. The Internet recognizes no geographical boundaries and does not follow the contours of national borders. This point is particularly salient when we consider a few facts: fewer than 15 percent of Internet users are American citizens; a large portion of the U.S. information technology and security workforce is composed of foreign nationals; and the supply chain for the global information technology market is not actually a chain but rather a complicated web involving many non-American actors. National security agencies within the U.S. government are ill-suited for managing such a domain by themselves. Indeed, their dominance of cyber security policy will render cooperation with international actors more difficult.

Toward a Balanced Cyber Security Policy

The United States needs a more balanced cyber security policy. Such an approach should include the following:

Focus on defense by building security in. A good offense is not a good defense. Instead a good defense is the best defense. A proper cyber defense involves building security into systems from the outset. The United States should invest greater resources in software security and solid security engineering. The U.S. government has an integral role to play in building more secure systems. Specifically, it should develop incentives for companies to engineer security into software rather than rely on endless patches after vulnerabilities become apparent. The U.S. government should consider granting tax credits to companies that develop more secure software. It should also publicize security failures to boost the situational awareness of companies and individual consumers.

There are literally thousands of ways in which better security engineering can help mitigate cyber risk. Border Gateway Protocol, one of the building block protocols of the Internet, is deeply broken and needs to be fixed. The vulnerabilities inherent to BGP illustrate our view that improved defenses through better security engineering is essential to attaining cyber security and keeping the cyber peace. If BGP were better designed, it would be more difficult to exploit and more difficult to mismanage accidentally.

People know how to build secure software. The commercial world, led by independent software vendors (think Microsoft, SAP, Adobe and Intuit) and financial services companies (think Bank of America, Wells Fargo and Goldman Sachs), has made great strides in software security over the last decade. The Building Security In Maturity Model (BSIMM) is designed to help understand, measure and plan a software security initiative.[22] The BSIMM carefully describes the work of 33 firms – all household names – responsible for building a majority of software in common use today.[23] The BSIMM was created by observing and analyzing real-world data and is designed to help a firm (or government agency) determine how its organization compares to other real-world software security initiatives and what steps can be taken to make its approach more effective. The most important use of the BSIMM is as a measuring stick to determine where a particular approach to software security currently stands relative to others.

Unfortunately, the U.S. government is drastically behind in software security. Not even the most advanced government agencies or contractors are ready for participation in the BSIMM project – mostly because there is nothing to measure.

Building more secure software is an important option because it kills three birds with one stone. Building security in will not only deter cyber crime and cyber espionage but it will also keep the cyber peace. Working to promote software security and security engineering is a considerably more viable response to cyber threat than blithely developing new offensive capabilities. In fact, shiny new cyber weaponry can be repurposed for crime and espionage – reason enough to pause before investing too much in offense.

Throwing a better, more accurate rock in a glass house is still throwing a rock. U. S. systems are so permeated with problems that even a relative amateur can exploit them – as a quick trip to the Black Hat hacker conference will show. To stretch the analogy a bit, if a cyber peashooter in the hands of a teenager is sufficient to wreak havoc on today's vulnerable systems, why bother to even work on a cyber rock?

Reorient Public-Private Partnerships. As it turns out, security is only partially a game of operations centers, information sharing and reacting when the flawed systems get exploited. (This is the cardboard shield defense.) Similarly, a focus on forensics assumes that an exploit has already happened and there is a mess to clean up.

Unfortunately, today's public-private partnerships focus overwhelmingly on information sharing and reacting collectively to cyber threats. There is nothing wrong with this approach, but it does little to help create fundamentally more secure systems. Public-private partnership discussions should be reoriented toward software security and building on the collective wisdom of many (as the BSIMM project does).

Focus on Information Users Instead of Plumbing. Civilian, government and military systems are deeply entangled. As the WikiLeaks episode demonstrates in no uncertain terms, the nature of the entanglement is the people who interact with the systems, not the technology, sets of wires or physical infrastructure. Although the U.S. government adopted some new security measures after WikiLeaks, there are still hundreds of thousands of users of classified government networks who also use the open Internet and carry around pen drives. Just as military and civilian social groups mix in complex and unpredictable ways in the physical world, so too do the information systems that these people use. The notion of building a "walled garden" to protect critical systems or classified information is thus misguided.

Instead of trying to construct new networks that exist in isolation, the U.S. government would do better to focus on the users. Thinking about who should access what information, when, where and why, and how much information should be accessed at once, are far superior to trying (and failing) to wall things off artificially.

Of course, the military has already attempted to separate certain networks with the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network (SIPRNet), systems of interconnected computer networks used to transmit classified information securely. The proposed "dot secure" network, which U.S. government officials have floated as a separate, secure computer network to protect civilian government agencies and critical industries, is basically the same notion, but intended to be used by critical infrastructure providers. However, there is an essential difference in purpose that we must point out.

The secret networks are for protecting state secrets, whereas "dot secure" is meant to protect against active attack. The current design of the SIPRNet and

JWICS allows information to transfer from low-to-high (from the open Internet "up" to SIPRNet, for example). Because of this feature – a feature that is accounts for most of the utility of the secret networks – the secret networks are susceptible to a malicious code infection that rides its way "up" on data. Deputy Secretary of Defense William Lynn's *Foreign Affairs* article shows that not only is this possible, but it has actually happened. The problem that this raises has everything to do with the different purpose that "dot secure" is intended for. A command and control system meant to stay up during an active attack has a completely different threat model and risk profile than a network to store and manipulate secrets.

Any Internet pundit familiar with Facebook knows that the value of a network is directly proportional to the number of people connected to it. By imposing limitations and constraints on a network, one degrades its value and utility. Make a network useless enough and users will go elsewhere or, worse yet, they will hack their way around security controls.[24]

Even if substantial taxpayer money and collective expertise is dedicated to the task of building better, more secure systems, successful attacks are still inevitable. Cyber security policy should be assume that risk cannot be completely avoided and systems must continue to function even in suboptimal conditions.

Let civilian agencies lead. The American government should not allow the National Security Agency (NSA) or another part of the intelligence community to dominate U.S. cyber security policy, for two reasons. The first has to do with separation of duties. Spycraft is facilitated by vulnerabilities in software that can be exploited in order to turn electronic devices into eavesdropping platforms. Consequently, an agency charged with spycraft understandably has mixed incentives to promote better software security.

The balance that the United States struck during the Cold War on nuclear policy may prove instructive here. Duties were separated between the Department of Energy – charged with building nuclear weapons – and the Department of Defense – charged with delivering them. This division has endured until today, and suggests that civilian agencies should take the lead on building cyber defenses while the national security establishment should focus on military dimensions.

An additional reason the intelligence community should not dominate cyber security is that important cultural differences exist between the national security community and the rest of civilian government and corporate America. There is a clearer command and control structure within the former than within the latter two. Though some ambiguity persists within the national security community, it is clearer who has to do what, and where the chain of command goes next. The same sort of clarity does not exist elsewhere. Put more colloquially, what seems to work for the NSA is very unlikely to work for Duke Energy, JP Morgan Chase or Microsoft.

Conclusion

In our view, cyber security policy must focus on solving the software security problem – fixing the broken stuff. We must refocus our energy on fixing the glass house problem instead of on building faster, more accurate rocks to throw. We must identify, understand and mitigate computer-related risks.[25] We must begin to solve the software security problem.

To date, when it comes to software, newly-minted Apple Chief Information Security Officer David Rice said it best in his book *Geekonomics*, "Unfortunately, the blunders of government are matched almost equally by the blunders of the market itself, if not more."[26] We believe that the government can and should play a role in building more secure systems. The U.S. government should develop incentives for vendors to build security in and break the endless loop of feature creep and bloatware. The government should publicize security failures so that we know what is really happening and we can learn from our mistakes. Perhaps the government should even grant tax credits for creating better, more secure software.

Equally important is what the government should not do. The government should not legislate cyber security excessively. The U.S. Computer Fraud and Abuse Act has done little to deter the explosive growth of cyber crime. Frankly, the target-rich environment filled with broken software makes it far too easy and too tempting to misbehave criminally. The government should not pretend that its buying power can single-handedly move the software market. It cannot. The government should not build any more overly bureaucratic taxonomies for security evaluation such as the Common Criteria or the Trusted Computer System Evaluation Criteria (TCSEC), a Pentagon standard that sets basic requirements for assessing a computer system's security control effectiveness. The market does not care.

When bits are money, the invisible hand will move to protect the bits. Of course, the invisible hand must be guided by the sentient mind and slapped hard to correct the grab reflex if and when it occurs. There is an active role for government in all of this, not just through regulation, but also through monitoring and enforcing due process and providing the right incentives and disincentives. In the end, somebody must pay for broken security and somebody must reward good security. Only then will things start to improve. Washington can and should play an important role in this process.

ENDNOTES

1. President Obama addressed cyber risk in an important address on cyber security and the national infrastructure. President Barack Obama, "Remarks By The President on Securing Our Nation's Cyber Infrastructure" (29 May 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

2. That standard issue distributed denial-of-service attacks are considered a bad joke among those in the technical know does little to frame or even inform the seriousness with which politicians approach the issue.

3. Brian Krebs, "Brazilian Govt: Soot, not hackers, caused '07 blackouts," *The Washington Post* (11 November 2009).

4. That is, injection bugs in Structured Query Language (SQL), a computer database language.

5. Agencia Nacional De Energia Eletrica, "Monitoring of the Blackout on November 10th, 2009" (26 March 2010), http://www.aneel.gov.br/aplicacoes/noticias_area/dsp_detalheNoticia.cfm?idNoticia=3338&idAreaNoticia=347.

6. For one of the worst offenders, see "Cyber Experts Have Proof That China Has Hijacked U.S.-Based Internet Traffic," *National Defense* (12 November 2010), http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249.

7. For the real numbers, see Craig Labovitz, "China Hijacks 15 Percent of Internet Traffic?" *Arbor Networks Security* (19 November 2010), http://asert.arbornetworks.com/2010/11/china-hijacks-15-of-internet-traffic/.

8. When pressed on the issue of mixing hyped stories with more severe attacks, Richard Clarke responds that he merely wants to put all the data on the table and let people decide for themselves. Gary McGraw discusses that point with Richard Clarke on *Silver Bullet Security Podcast* episode 50, http://www.cigital.com/silverbullet/show-050/.

9. Richard Clarke and Robert Knake, *Cyber War* (New York: Ecco, 2010).

10. Uzi Mahnaimi, Sarah Baxter and Michael Sheridan, "Israelis 'blew apart Syrian nuclear cache,'" *The Sunday Times* (London) (16 September 2007).

11. Gary McGraw, "How to p0wn a Control System with Stuxnet," *informIT* (23 September 2010), http://www.informit.com/articles/article.aspx?p=1636983.

12. For more on Stuxnet, listen to Gary McGraw interviewing Ralph Langner on *Silver Bullet Security Podcast* episode 59, http://www.cigital.com/silverbullet/show-059/. Note that there are millions of control systems currently vulnerable to Stuxnet-like attacks spread throughout the industrialized world.

13. William Lynn, "Defending a New Domain," *Foreign Affairs* (September/October 2010).

14. Greg Hoglund and Gary McGraw, *Exploiting Software* (Reading, MA: Addison-Wesley Professional, 2004).

15. Gary McGraw, *Software Security* (Reading, MA: Addison-Wesley Professional, 2006).

16. Verizon Business RISK Team, *2009 Data Breach Investigations Report*, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

17. David DeWalt, "Unsecured Economies – A Trillion Dollar Headwind," *McAfee Blog Central* (29 January 2009).

18. Ross Anderson, *Security Engineerin*g, 2nd ed. (Hoboken, NJ: Wiley, 2008).

19. Gary McGraw, "If You Build It, They'll Crash It," *Dark Reading* (7 July 2006), http://www.darkreading.com/security/application-security/208803559/index.html.

20. Note that software security is a relatively recent field in computer security with the first book published a little less than a decade ago. See John Viega and Gary McGraw, *Building Secure Software* (Reading, MA: Addison-Wesley Professional, 2001).

21. Siobhan Gorman and Yochi Dreazen, "Military Command is Created For Cyber Security," *The Wall Street Journal* (24 June 2009).

22. The Building Security In Maturity Model itself is available for free under the creative commons at http://bsimm.com.

23. Building Security In Maturity Model (BSIMM) companies who graciously agreed to be identified include: Adobe, Aon, Bank of America, Capital One, The Depository Trust & Clearing Corporation (DTCC), EMC, Google, Intel, Intuit, McKesson, Microsoft, Nokia, QUALCOMM, Sallie Mae, SAP, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, VMware and Wells Fargo.

24. For real-world examples of this phenomenon, see Gary McGraw and Jim Routh, "Lifestyle Hackers," *CSO Online* (2 November 2009), http://www.csoonline.com/article/506309/lifestyle-hackers.

25. Peter Neumann, *Computer Related Risks* (Reading, MA: Addison-Wesley Professional, 1994).

26. David Rice, *Geekonomics: The Real Cost of Insecure Software* (Reading, MA: Addison-Wesley Professional, 2007): 286.

Acknowledgment: Portions of this article are based on an earlier work by Gary McGraw and Ivan Arce, "Cyber Warmongering and Influence Peddling," *informIT* (24 November 2010).