SMALL WARS JOURNAL

THE CASE FOR CYBER

Articles

Thu, 09/13/2012 - 5:30am

Cyber warfare isn't hype; it's real. America's decisive technological advantage now contains the seed of our undoing. Our technological dependence is woven into the fabric of our way of life and our national defense. GPS satellites guide troops and weapon systems, algorithms fly aircraft and allocate supplies, websites drive personnel assignments and promotion boards, and official and personal data and voice communications almost exclusively transit computer networks. If these critical networks begin to fail, we aren't a twenty-first century fighting force; we are a 1980-era military. This estimate is generous. In 1980, we knew how to fight using face-to-face communications, manual land navigation, analog radios, and acetate overlays. Today is different. Information technology has largely kept its allure of dramatically increased efficiency at low cost. Thus, we no longer have "stubby pencil" warfighting skills or the extra personnel to handle these myriad manual tasks.

American society sits even more precariously. Over the past twenty years, we have gradually discarded the manual systems that ran our infrastructure, replaced by fragile, but more efficient automated systems. The lingering elements of our pre-Internet life—such as the Postal Service, paper currency, and land line telephones—are becoming extinct. Our entire economy is comprised of data stored in financial systems, as are our identities and the nation's crown jewel: intellectual capital. We aggressively chase technology's promised gains, such as smart electric grids, pilot-less

aircraft, electronic voting, and cloud computing. Technological dependence is ubiquitous. Ironically, while the average teenager has matured in a country where “online" is as commonplace as hot water (http://www.beloit.edu/mindset/2015/), technically-expert senior military leaders are scarce.

This paper will examine cyber warfare’s threat, clearly explain its import to the military professional, and suggest a way ahead. Stories of isolated security incidents surface daily, but are quickly forgotten. We thus seek to present a compelling case for cyber security that will garner informed support and motivate action within our military. This isn’t just a problem for communications and intelligence specialists. The cyber security problem we all face is unprecedented; we can only get it right through teamwork.

Cyber operations will occur in cyberspace, but what is “cyberspace?” We use the definition found in National Security Presidential Directive 54 (http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative): the “interdependent network of information technology infrastructures, [including] the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.”

The Threat Landscape

The following examples highlight the daily threat:

- This year researchers discovered (http://threatpost.com/en_us/blogs/researchers-find-sykipot-trojan-variant-hijacking-dod-smart-cards-011212) malicious software, circulating since 2011, that captures PIN numbers and hijacks DoD smart cards, allowing attackers access to CAC card protected systems.

- Disclosed in 2011, McAfee researchers uncovered a massive five-year hacking campaign, dubbed Operation Shady RAT (http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf), which infiltrated more than 70 companies, governments, and non-profit organizations in 14 countries.

- In 2011, NASDAQ officials discovered that their network contained software that spied on directors of publicly-held companies (http://www.reuters.com/article/2011/10/20/us-nasdaq-hacking-idUSTRE79J84T20111020).

- Iran may have used cyber capabilities to capture a US drone by jamming its GPS guidance system (http://www.foxnews.mobi/quickPage.html?page=38321&content=62659842&pageNum=-1) and the Air Force recently discovered a virus in the remote cockpits of its drone fleet (http://www.wired.com/dangerroom/2011/10/drone-virus-nuisance/). In 2009, militants used a $26 software package to capture Predator surveillance video (http://www.networkworld.com/news/2009/121709-drone-intercept-encryption.html). Currently almost 1 in 3 U.S. warplanes is a robot (http://www.wired.com/dangerroom/2012/01/drone-report/).

- RSA Security, a leading provider of cryptographic systems, was attacked in 2011; extremely sensitive information regarding its SecurID (http://www.wired.com/threatlevel/2011/06/rsa-replaces-securid-tokens/) system was stolen. This information likely facilitated successful follow-on attacks against major defense contractors (http://www.reuters.com/article/2011/05/27/us-usa-defense-hackers-idUSTRE74Q6VY20110527). Next generation weapon system plans were a probable target.

- As much as $1 trillion of intellectual property (http://www.economist.com/node/21532263) is stolen each year; some experts claim online crime revenues may now exceed the global drug trade.

- Also in 2011, attackers infiltrated Sony's massive online gaming network (http://online.wsj.com/article/SB10001424052748703849204576302970153688918.html) stealing personal information for approximately 100 million accounts.

- In 2009, Google disclosed (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html) it and at least 20 other companies were subject to a sophisticated attack (http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf) targeting the source code that underpins many sensitive systems.

- In the 2009 GhostNet compromise (http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=all), approximately 1,300 computers were infiltrated in 103 countries. Targets included embassies and government officials.

- In 2008, malicious software (http://www.wired.com/dangerroom/2011/12/worm-pentagon/) seriously compromised air-gapped classified military networks (http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain).

- In 2007, the Office of the Secretary of Defense's (http://www.informationweek.com/news/200000073) email system was compromised and thus forced offline to stem the damage.

These events presage a devastating cyber security event that threatens our way of life. An equally dangerous alternative is if thousands of cyber attacks sap American innovation and commerce without reaching the threshold to spur significant government response. Technology enables us to defeat a numerically-superior enemy. We have enjoyed information dominance since, at least, the Persian Gulf War. However, our adversaries—from lone malicious hackers and terrorist groups to organized online crime rings and nation states—are active in cyberspace and turning this greatest strength against us.

The nationwide investment in cyber security and the formation of U.S. Cyber Command and service component cyber commands signal a national awakening to this threat. In a 2009 address, President Obama argued that the "cyber threat is one of the most serious economic and national security challenges (http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure) we face as a nation." General Keith Alexander, Commander of U.S.

Cyber Command, stated that current DoD networks are “not defensible (http://www.wired.com/dangerroom/2012/01/nsa-cant-defend/).” During his confirmation hearings, Secretary of Defense Leon Panetta stated, “There is a strong likelihood that the next Pearl Harbor (http://www.nextgov.com/cybersecurity/cybersecurity-report/2011/08/panetta-invokes-pearl-harbor-while-anonymous-calls-for-revolution/54760/) that we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems. This is a real possibility in today's world.” We wholeheartedly agree.

No Easy Solution

The best defensive techniques might slow a determined adversary, but will ultimately fail. Ad hoc technical solutions aren’t the answer. Consider the following:

- Most military computing systems rely on distrusted components. In particular, America possesses a very limited capability to manufacture advanced microchips; rigorously validating foreign manufactured circuitry is impossible, except in small numbers (http://www.youtube.com/watch?v=IWGjWYIToFU). Additionally, adversaries can compromise a system anywhere along the supply chain (http://en.wikipedia.org/wiki/Supply_chain_security). Thus, many computing systems rest on a precarious foundation.

- A single trusted insider, turned bad, can have devastating consequences, particularly when empowered by today’s technology which enables rapid and high volume collection and dissemination of sensitive data. Consider the recent WikiLeaks debacle (http://www.politico.com/news/stories/1211/70826.html).

- Digital information is slippery. Divulged sensitive data is likely permanently compromised. For example, although Pentagon policies forbade DoD personnel from accessing WikiLeaks data, *already widely available on the Internet (http://www.wired.com/dangerroom/2010/08/pentagon-to-troops-taliban-can-read-wikileaks-you-cant/)*, they did little to curb global access.

- Antivirus systems are only a partial solution and cannot keep pace with rapidly evolving malicious software variations. A determined attacker can easily bypass (http://www.wired.com/threatlevel/2008/04/hacker-challeng/) antivirus protections. Powerful new exploits are available in underground markets (http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/) for about $100,000, sometimes for much less.

- A few vendors provide most of our hardware and software. Thus, targeting a single flaw can compromise countless machines.

- Isolated networks don’t guarantee security. Attackers have developed weaponized software that hops networks and patiently awaits inevitable security lapses, like the Stuxnet virus (http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs), which used USB storage devices to access sensitive systems.

- Security experts are in critically short supply. While initiatives to recruit, develop, utilize, and retain (http://smallwarsjournal.com/jrnl/art/recruiting-development-and-retention-of-cyber-warriors-despite-an-inhospitable-culture) qualified personnel continue, the military's kinetic warfighting culture may resist supporting these programs.

Severely dangerous problems span the spectrum of cyber security and cyberspace operations and are compounded by laws and policies that lag behind rapid technological advancements. Often combat is fought on the seams between two adjoining maps (http://www.murphys-laws.com/murphy/murphy-war.html); the same occurs in cyber warfare. Political and legal seams between governmental organizations provide opportunities to exploit our bureaucratic rigidity. One expert uses the following analogy: "Cyberspace is the only domain without a primary Service as lead and the only domain in which DOD will not defend the U.S. homeland. For example, if DOD defended the land domain in the same manner as cyberspace, a Russian land invasion of New Jersey would be fought by U.S. citizens and commercial entities with whatever weapons they happened to possess. DOD would only defend Fort Monmouth and Fort Dix (http://www.ndu.edu/press/USCYBERCOM.html)." Clearly we have a problem.

Three Facets of Military Vulnerability

Cyber warfare capabilities are quickly becoming a key weapon system–for us and for our adversaries. The popularity, effectiveness, and relatively-low cost of cyberspace weapon systems have spurred a silent cyber arms race (http://www.mcafee.com/us/about/news/2012/q1/20120130-02.aspx). To better understand the critical implications of cyber warfare specific to the military, we consider three areas: personal computing devices, garrison computer systems, and deployed computing systems.

At Home

American service members have traditionally considered the homeland as safe. However, we may be more vulnerable in the cyberspace domain when using personal electronic devices. Personal computers don't just contain personal information. Many service members work on home systems rarely managed to the same standard as military platforms and networks. Home devices are thus far softer targets. While modern operating systems are notably more secure than their predecessors, and free antivirus software is available to service members, every system remains vulnerable.

Social networking sites such as Facebook and LinkedIn compound this risk, as service members and their families disclose sensitive personal information useful for targeted attacks (http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/). Home and public wireless hotspots are notoriously insecure (http://dl.acm.org/citation.cfm?id=1132501); emerging commercial technologies, such as wireless capability for automobiles, provide new attack vectors (http://cacm.acm.org/magazines/2011/11/138210-hacking-cars/fulltext). The security lapses of family members, including web-surfing children, jeopardize entire households. A service member's typical home environment is thus easily targeted by even a poorly-resourced attacker, let alone skilled and determined adversaries.

In Garrison

Free from combat's kinetic threats, garrison life involves training for and recovery from armed conflict. Networks and workplace computers are professionally managed using baseline system configurations (http://www.army.mil/article/21389/army-migrating-computers-to-vista/) such as Army Golden Master and the Host Based Security System (http://www.disa.mil/Services/Information-Assurance/HBSS) (HBSS). But no computer system is hack-proof. Phishing attacks are one viable threat. For example, service members, their families, and veterans were recently subject to a phishing attack (http://www.army.mil/article/71306/) using fake emails purporting to come from a popular financial services company. The emails tricked recipients into opening an attachment that would initiate malicious software. An ongoing challenge (http://smallwarsjournal.com/jrnl/art/the-militarys-cultural-disregard-for-personal-information) is the widespread use of personal information to validate user access to official websites and as an easily accessible identifier on many military forms despite concerted efforts to curb the problem. In 2011, TRICARE announced a massive breach of personally-identifiable and protected health information impacting nearly 5 million military medical patients. Also in 2011, Pentagon Federal Credit Union admitted (https://threatpost.com/en_us/blogs/infected-pc-compromises-pentagon-credit-union-011211)that unauthorized access to members' names, addresses, and account information occurred due to an infected laptop. Gannett Government Media, publisher of the *Army Times*, was successfully attacked (http://latimesblogs.latimes.com/technology/2011/06/army-times-defense-news-and-other-gannett-government-media-websites-hacked.html), compromising personal details of "some users." Even the military's CAC system, the backbone of authenticated access, is vulnerable. In 2012, the Army Times reported a Chinese virus that specifically targeted DoD CAC card users (http://www.armytimes.com/news/2012/01/military-common-access-card-chinese-virus-011812w/) to access "official use only" files. Garrison systems present a more difficult, though surmountable, target for attackers.

In Combat

In combat, the military takes extensive force protection measures to protect against kinetic and cyber attack. However, the pressures of life in a combat zone inevitably force users to weigh the immediacy of mission accomplishment against far less concrete cyber risks. For example, widespread use of USB thumb drives introduced malicious software into DoD systems and lost drives have surfaced in local bazaars (http://articles.latimes.com/2006/apr/10/world/fg-disks10). Combat operations require access to sensitive data, and trust is implicit. Unfortunately, the threat of a malicious or non-malicious insider threat remains present. While malicious insiders are thankfully rare, myriad well-intentioned service members, contractors, and allies cut corners due to perceived need for expediency.

Malicious software is always pernicious, but deployed forces are particularly vulnerable. MWR facilities risk hosting shared community computers. Foreign shops offer cut-rate bootleg software and movies, sometimes with malicious surprises. The intensity of deployment diverts service members' attention away from personal matters back home, making them more vulnerable to

identity theft and fraud (http://smallwarsjournal.com/jrnl/art/the-militarys-cultural-disregard-for-personal-information). Their families are likewise open to service-related scams, as criminals steal identities of deployed service members.

Ideal tools for information sharing, mobile devices also pose threats. The Army intends to issue smart phones (http://www.armytimes.com/news/2011/12/army-expects-to-field-smartphones-next-year-122911/) to soldiers for use on the battlefield. While this initiative may have many benefits, these devices will pose a constant concern. Consider the Abu Ghraib (http://www.newyorker.com/archive/2004/05/10/040510fa_fact) photographs or Marines' urinating (http://www.huffingtonpost.com/2012/01/13/marines-urinating-on-taliban-identified_n_1204653.html) on a Taliban corpse: easily-accessible information technology can yield unintended consequences.

Military robotic systems are also proliferating. These systems depend on their command and control links and their associated algorithms and computers. While hardened against attack, they still pose risks. In this context, cyber security is increasingly critical lest our powerful weapon systems be turned against us. Vulnerabilities may come from the myriad commercial off-the-shelf components comprising these systems, from designs stolen from defense contractors or from the failings of those working with these systems.

Way Ahead

This article would be incomplete without solutions. In this section we offer five objectives as a way to support both national and personal security.

Establish a Sense of Urgency

We must embark upon a major transformation to maintain technological supremacy. In effect, we are in step one of Kotter's eight-step change management process: "establishing a sense of urgency (http://hbr.org/2007/01/leading-change-why-transformation-efforts-fail/ar/1)." Therefore, we must identify and examine the challenges and encourage open communication.

The cyber threat is real; the potential impacts, omnipresent. To affect change, we must abandon the current lens we use to view cyber: many still see it as the IT department's hobby horse. It is everyone's responsibility because it affects not just our email or access to routine documents, but also our defense supply chain and weapon systems. It threatens our national security.

Fundamental change must be part of our daily discourse. We should discuss the protection of sensitive data at work and home, read privacy statements, and ask financial institutions about safeguarding personal data. We should ask questions about our most vital weapon systems' vulnerabilities. When leaders show genuine concern for cyber issues, people will respond and change will begin. Cyber security is fundamentally a leadership issue.

Understand Cyber Concepts and Challenges

Today's youth will likely understand cyber concepts better than us—these digital natives already rely on technology for education, news, entertainment, transportation, and social satisfaction. Many senior leaders did not have personal computers until after college graduation. Likewise, even some of our mid-grade officers lack a basic grasp of cyber concepts, despite their deeper exposure to technology. A common lexicon and understanding of cyber challenges is crucial; we must develop ourselves (http://smallwarsjournal.com/jrnl/art/self-development-for-cyber-warriors) and our subordinates (http://smallwarsjournal.com/jrnl/art/leadership-of-cyber-warriors-enduring-principles-and-new-directions) to be cyber savvy.

We already implement risk management, so applying it to cyber is natural. Leaders should understand the vulnerabilities of, and the threats to, our networks and systems. We should also know when and how to apply technology; sometimes it's better to use manual systems instead. Once we understand the risk, we can mitigate the threat. Everyone involved in defense needn't have a graduate degree in cyber security; but we critically need more than two hours of annual training.

Likewise, we must incorporate cyber threats into training exercises. Commanders and exercise planners have been previously reluctant to insert cyber play because the effects might disrupt an exercise's kinetic objectives. As leaders, however, we must ensure our military is trained to operate with varying degrees of degraded network functionality. Though the most technologically-advanced military in the world, can we operate without our gadgets? We should candidly assess our limitations, however painful, and then minimize them. Cyber is an inherent component of warfighting; failing to train as we fight puts us all at risk.

Defend Against Cyber Threats

Cyber defense is inherently problematic because the Internet operates on the principle of openness. Organizational tension always exists between information accessibility and security. We should expect intrusions and learn to respond decisively by isolating breaches and recovering quickly. This requires constant monitoring and coordination at all command levels. Responses to cyber threats may need to occur at speeds beyond human capacity; thus, automated defensive systems are crucial.

We must also support our unit-level defenders by cooperating with requests for information and not circumventing security mechanisms. Most cyber-related intelligence is highly-classified, so we are rarely privy to the whole story. Everyone must know cyber-attack symptoms and understand incident response procedures, so cyber battle drills must be published and rehearsed. Mistakes will happen, but when we find malicious insiders intentionally perpetrating cybercrimes, we must police our own. We should likewise underwrite honest mistakes and use such occurrences to better educate our organizations.

Defending home computers can be improved, but not guaranteed, by following a few simple rules. We recommend NSA's "Best Practices for Keeping Your Home Network Secure (http://www.zdnet.com/blog/hardware/are-you-following-the-nsas-home-network-security-best-practices/12589)." Additionally, since malicious hackers exploit human weaknesses, they will use

social engineering to dupe their targets. We must protect our personal information. Keep life stories off social networking sites lest attackers obtain the information needed to guess passwords, gain access to important accounts, or employ targeted phishing or social engineering attacks.

Shape the Development of Military Doctrine, Organizations, and Strategies

Cyber Operations is in its infancy. We all can shape our future organization. There's much work to be done nationally to identify appropriate organizational constructs across the federal government, with state and local partners, and with private industry. Some military organizations responsible for operating and defending the cyberspace domain have barely articulated their mission statements, so we should collectively discuss structures, doctrine, and strategies crucial for success.

We should smartly leverage existing talent found in academia, industry, non-profits, and the hacker community, remembering the multifaceted nature of the cyberspace domain. Improving the processes and technology to defend our networks won't suffice. We must better understand how weapon systems—tanks, airplanes, ships, and satellites—think and function, which requires cooperation with organizations and people outside the usual defense industrial base.

Manage the Cyber Workforce

People are the key, so we must define and cultivate an elite cyber workforce. Fortunately, progress is ongoing. As an example, the National Initiative for Cybersecurity Education (NICE) leadership plan identifies 43 different skills in seven cyber-related areas. Human resource professionals should recognize these newly-defined skills and create new military and civilian career paths.

Our existing workforce can learn new skills, but our future rests with tomorrow's leaders. In raw numbers, we are demographically and culturally disadvantaged: China has more honors students than we have students (http://blow.blogs.nytimes.com/2008/07/31/they-have-more-honors-kids-than-we-have-kids/), and America's youth rank dismally low (http://www.bizjournals.com/seattle/stories/2008/06/23/editorial3.html?page=all) in math and science compared to other industrialized countries. Our schools must revitalize Science, Technology, Engineering, and Math (STEM) programs. We must foster the emerging cyber warrior's lifespan, from early identification and nurturing to career-long professional development in the military and through post-military service. As we nurture this cyber workforce, we must incentivize existing talent to support our national objectives.

Conclusions

We have become desensitized to daily news of computer security lapses. Today we witness an increase in attacks ranging from minor inconveniences to cyber events arguably akin to acts of war. Whether these battles are fought through proxies or by nation-states, cyber warfare escalation is here, and we must take it seriously. But cyberspace operations can also provide us unprecedented advantage. Leaders of all military ranks must facilitate the necessary change forced upon us by this man-made operational domain. Our nation's landscape and modern warfighting have fundamentally changed.

We have painted a candid picture of the challenges we face in the cyberspace domain. The promise, potential, and ever-presence of cyber are undeniable: it touches nearly every facet of our lives. Today's decisions will shape our nation's prosperity, our military's strength, and the quality of our children's lives. Cyber is not simply a one-off problem, like the Y2K bug, but instead represents a fundamental shift in warfighting. We have the opportunity to do it right, but the change required will take considerable debate, cooperation, and ultimately, decisive action.

The views expressed in this article are the authors' and do not reflect the official policy or position of West Point, Army Cyber Command, Department of the Army, Department of Defense, or US Government.

Categories: network protection (/taxonomy/term/1151) - network (/taxonomy/term/1152) - information security (/taxonomy/term/675) - information assurance (/taxonomy/term/206) - cyberwarfare (/taxonomy/term/834) - cyber (/taxonomy/term/369)

About the Author(s)

Gregory Conti (/author/gregory-conti)

Colonel Gregory Conti is a Military Intelligence Officer and Director of West Point's Cyber Research Center. He holds a Ph.D. from the Georgia Institute of Technology, an M.S. from Johns Hopkins University and B.S. from West Point. He has served as an advisor in US Cyber Command Commander's Action Group (CAG), as Officer in Charge of US Cyber Command's Expeditionary Cyber Support Element in support of Operation Iraqi Freedom, and co-developed US Cyber Command's Joint Advanced Cyber Warfare Course.

John Nelson (/author/john-nelson)

Colonel John Nelson is a Signal Officer and an Academy Professor in the Department of English and Philosophy at West Point. Colonel Nelson has a Ph.D. from the University of Washington, an M.A. from Oregon State University, and a B.S. from West Point.

Jacob Cox (/author/jacob-cox)

Major Jacob Cox is a Telecommunications Engineering Officer and Information Technology Instructor for West Point's Department of Electrical Engineering and Computer Science. He holds an M.S. from Duke University and a B.S. from Clemson University. He has served in communication-related positions in U.S. Army Training Command and 2nd Infantry Division.

Jon Brickey (/author/jon-brickey)

Lieutenant Colonel Jon Brickey is an Information Systems Officer and the Army Cyber Command Fellow at the Combating Terrorism Center, West Point. He holds a B.S. from West Point, an M.S. from the Naval Postgraduate School, and a Ph.D. from the University of Colorado Denver. He has held leadership positions in cyber-related programs at the National Security Agency, USNORTHCOM, and USARCENT.