Introduction

In response to increasing cyber intrusions, the United States government has exponentially strengthened its investment in cyber defense capabilities over the past decade. In just two years, Congress introduced over 90 bills related to cybersecurity through four different Committees and former President Obama directed five executive orders, supplementing his proposal to raise the fiscal year 2017 budget for cyber defense by 35% to $19 billion.

There are two competing arguments regarding the gravity of the threat that cyber-attacks pose to the nation’s security. On one hand, cyber-attacks present a serious national security threat that can cause as much harm as conventional military attacks, warranting a robust cybersecurity policy (cyber threat theory). Alternatively, cyber-attacks present a nuisance primarily to businesses and do not pose an imminent threat to the survival of the United States, causing the U.S. to overinvest in this area (cyber threat inflation theory).

An inquiry into the plausibility of future cyber war underlies this debate. In the Journal of Strategic Studies, dozens of experts have engaged in this discussion with articles that argue whether “Cyber War Will Take Place,” or whether “Cyber War Will Not Take Place.” Examining arguments on both sides of the debate provides policymakers and practitioners a basic framework for analyzing this increasingly salient national security issue. Such analysis necessitates an acknowledgement that sophisticated cyber operations are being orchestrated by individuals and groups who do not fit the stereotypical narrative of the 400-pound hacker, as President Donald Trump once suggested.

Cyber threat theory contends that cyber-attacks are emerging national security threats that may cause as much harm as conventional military tactics. U.S. policy tends to reflect this threat assessment.

By nature of cyberspace, efforts to attribute responsibility for cyber-attacks to states, rather than criminals or terrorists, often prove fruitless. This accountability problem hinders states’ ability to deter enemies who directly or indirectly perpetrate cyber-attacks without fear of legal liability or military response. Despite recent efforts by scholars to form international cyber norms through the creation of the Tallinn Manual, major geopolitical powers lack consensus on cyber norms which increases the likelihood for miscommunication, escalation, and potential crises. For example, one country can hack into another state’s system as benign “standard operating procedure,” but mistakenly leave an implant in a system marginally connected with critical infrastructure, prompting a disproportionate response. The increase of cyber offensive capabilities in China, Russia, and the U.S. have induced characterizations of a “quasi-arms race.”

Three notable incidents in the last decade demonstrate different methods through which cyber-attacks can pose a substantial threat to a nation’s security.

*Weakening Government Capabilities: The Bronze Statue incident in Estonia*

In 2007, distributed denial of service (DDoS) attacks targeted Estonia’s infrastructure and shut down the websites of all
government ministries, two major banks, and several political parties. Most have attributed blame to digital activists (also known as hacktivists). Although authorities arrested one individual, they never uncovered the primary culprits. This incident demonstrates that sophisticated political hacktivists may possess the ability to disrupt or destroy government operations. They can hide behind layers of software by manipulating globally dispersed and virtually untraceable computers (i.e. botnets) to execute the attacks.

**Augmenting Traditional Warfare: The Russo-Georgian War**

Prior to and during the Russo-Georgian War of 2008, Russia deployed decentralized cyber mobs to attack Georgia's infrastructure. These attacks blocked the ability of Georgian citizens to obtain information, disrupted access to banking for 10 days, and hindered Georgia's ability to mobilize an effective domestic and international response. This incident depicts how the digitization of government and military systems revolutionizes conventional warfare, particularly in the air and sea domains. Cyber warfare impacts engagement systems at the tactical level, the adversary's ability to mass and synchronize forces at the operational level, and the ability of senior leadership to maintain clear situational awareness of the national security environment at the strategic level. While cyber weapons do not have a direct kinetic effect, they can indirectly render defense systems, command and control (C2) systems, tanks, and aircraft useless. For example, Israeli cyber-attacks in 2007 spoofed Syrian air defense systems, enabling F-15 and F-16s to penetrate the airspace and destroy a suspected nuclear site. Similarly, Iranian cyber engineers, in conjunction with Russian assistance, brought down a valuable U.S. drone in 2011 by hacking global tracking systems.

**Threatening Critical Infrastructure: Stuxnet worm attack against Iran**

In 2009, *Stuxnet* – an alleged Israeli-American created virus – rendered Iranian nuclear centrifuges useless by making them rotate more rapidly in a suicidal-mechanical fashion. The type of malware associated with *Stuxnet*, now called *Duqu*, uses a coding platform that puts together different pieces of modules to create entirely different malware, surpassing the air-gap that exists between the internet and the system. This instance shows that cyber-attacks can pose debilitating physical effects by taking advantage of zero-day vulnerabilities and self-replicating itself among systems. A single cyber weapon can steal information from civilian institutions to create additional cyber weapons in a “cascading effect” that harms aircraft, air defense systems, and critical infrastructure. Industry leaders and congressional representatives frequently warn that the supervisory control and data acquisition (SCADA) systems underlying the nation's critical infrastructure possess potentially catastrophic vulnerabilities.

In sum, cyber threat theory contends that cyber-attacks pose a dangerous threat to national security by infiltrating government systems, complicating warfare, and attacking critical infrastructure.

In contrast, cyber threat inflation theory argues that cyber-attacks pose a nuisance primarily to contractors, enabling them to profit from inflated perceptions of cyber vulnerability.

Critics of cyber threat theory argue that most cyber-attacks fall below the threshold of armed conflict and do not threaten the defense capabilities of the U.S. Instead, they believe most so-called cyber-attacks are better characterized as criminal acts and cyber thefts. In a comprehensive study of 111 cyber incidents from 2001-2011 between rival states, scholars Brandon Valeriano and Ryan Maness found that only 20 out of 126 rival pairs of states engaged in government targeted conflicts and most of them tend to be mild nuisances and disruptions. According to the U.S. Government Accountability Office, only 18% of 44,562 cyber incidents directed at federal agencies resulted from malicious code, 17% from unauthorized access and the rest from improper usage, probes, and other benign intrusions. Rather than agitating geopolitical balance, the scholar, Thomas Rid, proposes that cyber-attacks will “diminish rather than accentuate political violence” by offering states and other actors a new mechanism to engage in aggression below the threshold of war.

If most cyber incidents comprise espionage cases that do not threaten the nation's security, it follows that public and private leaders hold an alternative reason for exaggerating cyber threats: lucrative government contracts. A strong qualitative and quantitative relationship between cyber defense investment and companies' revenue streams supports this cyber threat inflation theory.

**Defense budget cuts, accompanied by an exponential growth in the international cybersecurity market, has spurred private contractors to provide government cyber services.**

The global cybersecurity market has grown roughly 35 times in the last 13 years. Private sector firms own 85% of U.S. critical infrastructure assets and serve as the "de facto providers of software used by everyone," especially the federal government. During this period, traditional defense contractors, who are normally known for developing military weapon systems, have begun to create and expand their own cybersecurity centers. BAE Systems has purchased at least 9 cyber-related firms since 2005 and Boeing has spent over $1 billion doing the same since 2010. In May 2016, the United States Cyber Command (USCYBERCOM) awarded spots on a massive $460 million operations contract to 6 traditional contractors. The nature of this relationship has led several scholars to suspect excessive, unaccountable spending by the government. Like the “military-industrial complex,” this relationship can otherwise be known as the “cybersecurity-industrial complex,” the close nexus between the Pentagon, defense contractors, and elected officials that could lead to the unnecessary expansion of cybersecurity spending and a breakdown of checks and balances. Prior to a 2007 House oversight bill, the Office of the Director of National Intelligence allocated billions of dollars in classified intelligence work to contractors without having to inform Congress.
Parallel to general trends in the defense industry, budget constraints resulting from the end of the Cold War increased the pressure on the National Security Agency (NSA) to outsource their capabilities. Hiring close to 20 companies in the mid 1990's, the agency exponentially increased hiring to about 1,000 in 2002, 2,690 in 2004 and over 5,400 in 2008.27 Former high-ranking government and military officials have left their posts and accepted senior positions with military contractors, consultancies, and private-equity firms, often replicating the services they provided while in government.28 This revolving door of cyber-intelligence leaders gives them disproportionate influence in Congress and possibly taints the contracting decisions they made while serving. Today, approximately 1,500 companies lobby for Congress on cybersecurity issues, compared to just four in 2006.29 Historically, legislators tend to reject cybersecurity proposals that industry lobbyists do not approve of. As a major donor to both political parties since 1998, Microsoft has exercised such influence by convincing government agencies to use their software to reduce costs.30 After weaknesses were repeatedly exploited, the government considered a shift to cheaper, open-source software like Linux, but Microsoft successfully "went on the warpath" to retain their contracts.31

Heighed perceptions of cyber threats closely correlate with substantial increases in contractors' revenue, which indicates overriding economic interests.

The post 9/11 consensus on countering global terrorism accelerated the government's initially modest investment in the cyber industry. Created shortly after the attacks, the Bush administration created the Department of Homeland Security (DHS) in 2002 and shortly increased its "information analysis and infrastructure protection" spending by 370% in 2004.32 Meanwhile, total federal government spending in the informational technology sector increased by 9.7% to $53.1 billion in 2003, amounting to one-third of the entire industry's business.33 Following this money trail has led some scholars to conclude that threat inflation, similar to that witnessed during the build-up to the Iraq War, has driven the recent cyber defense splurge.34 The most widely cited literature in support of cyber investment, the 2008 Center for Strategic and International Studies Commission report and the best-selling book, Cyber War, predominantly utilizes unverifiable claims and anecdotal evidence.35 Speculative science is hardly the sort of information that should justify billions of American tax dollars. At congressional hearings, advocates who warn politicians of potentially catastrophic cyber threats often represent companies such as McAfee Corporation with decades-old government contracts.36

Conclusion

The cyber threat theory and cyber threat inflation theory present two opposing viewpoints of a prominent national debate. Like most complex subjects, the truth often falls in the middle of two extremes. Cyber-attacks potentially pose debilitating effects on critical infrastructure and the government's ability to wage war; their sophistication and potency outpace the development of cyber defense. Yet, the Estonian and Georgian examples demonstrate that cyber war will likely not occur unless it stems from an existing conflict escalated through conventional means.

While recognizing that cyber intrusions falling the below threshold of warfare can “snowball” into a bigger conflict and give the aggressor a conventional warfare edge, policymakers should not dictate cybersecurity policy based principally on doomsday scenarios. Such threat inflations, driven by the cybersecurity-industrial complex, causes the government and military to overspend on cyber systems. Instead, a nuanced knowledge of cybersecurity that properly accounts for political and financial scenarios. Such threat inflations, driven by the cybersecurity-industrial complex, causes the government and military to overspend on cyber systems. Instead, a nuanced knowledge of cybersecurity that properly accounts for political and financial incentives should drive the nation's investment decisions in cyber defense. Moving beyond the 400-pound hacker narrative, policymakers should focus on deep and intricate networks of state and non-state sponsored hackers who engage in cyber criminality, espionage, and other intrusions that degrade the ability of the military to operate in all of the combat domains.

End Notes


18. For a comprehensive chart of these findings, see page 88 of Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford UP, 2015. Also, WIRED's Ryan Singel reports in "White House Cyber Czar: 'There Is No Cyberwar.'" that Howard Schmidt, a cybersecurity adviser to former President Obama, said "there is no cyberwar" and that the government needs to focus its effects on online espionage.


26. ibid.  
27. ibid.  
28. ibid.  
30. Amitai Etzioni, "Cybersecurity in the private sector: the nations businesses manage a significant share of online activity related to national security and must play a larger role in ensuring the overall integrity of the system." Issues in Science and Technology 28.1 (2011): 60-61.  
31. ibid.  

Works Cited


26. ibid.  
27. ibid.  
28. ibid.  
30. Amitai Etzioni, "Cybersecurity in the private sector: the nations businesses manage a significant share of online activity related to national security and must play a larger role in ensuring the overall integrity of the system." Issues in Science and Technology 28.1 (2011): 60-61.  
31. ibid.  
Panetta, Leon E. “Defending the Nation from Cyber Attack” (Business Executives for National Security. New York, NY, 11 October
2012.


Categories: cyber warfare - cyber threat - cyber

About the Author(s)
Kenneth Mok currently works at the New York County District Attorney's Office. He earned a B.A. in Political Science and Economics from Northwestern University, and will be attending law school in 2018. He would like to thank Major (USAF) Jahara "FRANKY" Matisek for his guidance on this article.

RECENT HEADLINES

- Venezuela Prepares for More Protests Over Electricity Rations by VOA News
- On Central American Aid, Trump Is Half Right by Anita Isaacs and Anne Preston - NYT
- Kim Jong-nam Murder: Vietnamese Woman Pleads Guilty to Lesser Charge by BBC News
- Brunei to Enforce Stoning for Adultery, Gay Sex; Conservative Shift in Muslim Parts of Southeast Asia by Jon Emont - WSJ
- Pentagon Suspends F-35 Fighter Jet Deal With Turkey by Wall Street Journal
- Mozambique Races to Contain 1,000 Cases of Cholera by Associated Press
- Facebook Removes Hundreds of Fake Accounts Ahead of India Elections by Newley Purnell - WSJ
- Japan Names New Imperial Era 'Reiwa,' Symbol of the Country's Hopes for the Future by Simon Denyer - WaPo
- Algeria Protests: President Bouteflika to Quit Before 28 April by BBC News
- Algeria's Ruler, Abdelaziz Bouteflika, Agrees to Step Down by Adam Nossiter - NYT
- Turkey Elections Loosen Erdogan's Grip on Power, With Losses in Ankara, Istanbul by David Gauthier-Villars - WSJ
- Chinese Dissidents Feel Heat of Beijing's Wrath. Even in Canada. by Catherine Porter - NYT
- Parliament Aims to Break the Political Stalemate on Brexit by William Booth and Karla Adam - WaPo
- Erdogan, Turkey's Leader, Staring at Major Electoral Defeat by Carlotta Gall - NYT
- Brexit: MPs Debate Next Steps Ahead of Indicative Vote by BBC News
- Raleigh, NC: Army Special Ops Exercise Spooks Nearby Residents, City Officials Promise it Won't Happen Again by Kyle Rempfer - Military Times
- UK Parliament Votes on Brexit Options by Max Colchester - WSJ
- Whistleblower Says 25 Security Clearance Denials Overturned During Trump Administration by Rachael Bade - WaPo
- Mexican President Wants to 'Bring Order' to Central American Migration to US by Reuters
- The Future of Urban Warfare in the Age of Megacities by Rita Konaev - IFRI
- Turkey Says S-400 Delivery Talks Still On, Despite US Bill to Block F-35 by Joe Gould - Defense News
- Trump, Putin and a Possible 'Red-Line Moment' in Venezuela by David E. Sanger - NYT
- Book Review - "Japan Rearmed: The Politics of Military Power" by Sheila Smith by Catherine Putz - The Diplomat
- Congress to Pentagon: Um, We Asked You to Buy Tech Faster by Kelsey D. Atherton - CSISRN
- Two Pilots Killed in Marine Corps Helicopter Crash in Arizona by Associated Press
- 11 April - Youth: The Missing Peace by US Institute of Peace
- Afghan National Security Chief Is Sidelined in His Own War by Rod Nordland and Mujib Mashal - NYT
- No, Islamic State Isn't Defeated by Bloomberg News Editorial
- With Removal of IS, Syrians Search for Missing Loved Ones by Nisan Ahmado - VOA News
- Venezuela Crisis: Opposition's Guaidó Awaits Army Support by BBC News
- How Well Has Rwanda Healed 25 Years After the Genocide? by The Economist Editorial
- Report Says Algeria’s President Is Preparing to Resign by Associated Press
- Turkey Local Elections: Setback for Erdogan as His Party Loses Capital by BBC News
- Venezuela: Maduro Announces 30-Day Electricity Ration Plan by VOA News
In this post I will share the code snippet I am using to create pretty little share buttons for sharing my posts on Twitter, Facebook and Google Plus. I will also show how you can extend it to add more services like Reddit, LinkedIn, Tumblr etc. In order to add share buttons to my posts, I used the share URLs of the social networking sites such as Twitter, Facebook and Google Plus which simply use the GET parameters passed with the URL to create the share dialog. Step 1: Partial include file for share buttons.