Cyberdefense: *Is Outsourcing the Answer?*

by Kellen Ashford

Speaking at an event for the American Enterprise Institute in 2012, retired General Keith Alexander, the former head of U.S. Cyber Command and Director of the National Security Agency, suggested that "cyber crime is the greatest transfer of wealth in history."[1] The commercial cost of cyber crime is debatable, but General Alexander cited two figures, provided by Symantec and McAfee, that cyber crime costs U.S. companies $250 billion a year and $1 trillion a year globally. While these are estimates, the U.S. weapons systems linked to Chinese cyberespionage not only represent a significant transfer of dollar costs, but also associated military capability. In the non-public version of the Defense Science Board's report, "Resilient Military Systems and the Advanced Cyber Threat," the F-35 Joint Strike Fighter, Littoral Combat Ship, Aegis Combat System, and THAAD missile defense systems were among those whose designs have been compromised by Chinese cyberespionage campaigns. While the Chinese and other attackers pilfer contractor networks for intellectual property, they are also able to map Defense Department networks. For example, during the Chinese cyber campaign against QinetiQ North America, hackers were able to infiltrate the U.S. Army's Aviation and Missile Command.

Traditionally, former Cold War rival, Russia was viewed as the main threat to U.S. cybersecurity. In 2007, Estonia, often referred to as "e-Stonia" in technology circles, experienced "distributed denial of service" (DDoS) attacks that affected the government and financial industry. In an April editorial in *The New York Times*, Toomas Hendrik Ilves, President of Estonia, does not attribute blame for the attacks; however, initial suspicions and blame were cast at Russia. The cyberattacks took place after the Estonian government decided to move the Soviet-era "Bronze Soldier of Tallinn," which was followed by riots from ethnic Russians. Following the DDoS attacks, Estonian

Kellen Ashford is a graduate student at the University of Kansas. Formerly a student of political science, Ashford became interested in cybersecurity while working with clients in the defense and aerospace industries. This essay was written prior to Edward Snowden's leaks on the NSA became public knowledge, during Ashford's internship at the Simons Center.

Prime Minister Andrus Ansip suggested that the attacks originated from "Russian state authorities."[2]

While Russia remains a threat to U.S. cybersecurity, both countries have signed a cybersecurity pact aimed at reducing tensions between the two in cyberspace.

While Russia remains a threat to U.S. cybersecurity, both countries have signed a cybersecurity pact aimed at reducing tensions between the two in cyberspace. The pact calls for increasing communication and information sharing on cyber threats, as well as forums aimed at broadening cybersecurity cooperation.[3] In contrast to the perceived Russian cyberthreat, recent government and media attention has focused on cyberattacks and cyberespionage campaigns waged by Chinese hackers, and rightly so. Verizon's "2013 Data Breach Investigations Report" found that 96 percent of cyberespionage campaigns originated in China.[4] In early 2012, Mandiant, a cybersecurity company, released a report that linked cyberespionage to Unit 61398 (also called the Comment Crew or APT1), a division of the People's Liberation Army (PLA). Additionally, Chinese universities have also been linked to cyberattacks on the U.S. The Key Laboratory of Aerospace Information Security and Trusted Computing at Wuhan University, which receives funding from the PLA, has been linked to cyberattacks, and over 760 Chinese military and government officials are reported to have connections to the university.[5]

While critical infrastructure, government, and military networks remain at the center of cybersecurity concerns, the defense contracting community has been thrust onto the front lines of the cyberwar. Not only are the contractors' weapon systems subject to intellectual property theft, but they are also becoming the first responders for the U.S. government. In order to better secure their networks, defense contractors have taken both defensive and offensive measures against these cyberthreats. "Active defense," "hacking back," and "threat intelligence" are being discussed more frequently, if not becoming common offensive and defensive measures. The Commission on the Theft of American Intellectual Property, led by former Director of National Intelligence Admiral Dennis C. Blair and former Ambassador to China Jon Huntsman Jr., released a report which suggested that companies be allowed to "hack back" against hackers. Furthermore, Jim Jaeger, Vice President of General Dynamics Fidelis Cybersecurity Solutions, recently suggested that "if a company wants to go after a cyber criminal who is responsible for a security breach, who is going to complain? The hacker? Frankly, I think it's really good to see."[6]

Cyberattacks and cyberespionage are likely to continue against private and public networks in the U.S. and cyberdefense remains a priority. While the National Security Agency and defense contractors engage hackers with offensive measures, the need to defend America's networks has never been greater. Yet, in order to understand the importance of cyberdefense in the modern age, it is also important to understand the threat—in this case—Chinese hackers. While media attention continues to focus on how hackers attack and what their specific targets are, the bigger question is why the Chinese wage cyberespionage campaigns against defense contractors, the U.S. government, and critical infrastructure.

"The culture of hacking in China is not confined to top-secret military compounds where hackers carry out orders to pilfer data from foreign governments and corporations. Hacking thrives across official, corporate, and criminal

worlds."[7] Understanding the cyberthreat posed by the Chinese is to understand China, its history, and its intentions on the global stage. In his book, *21st Century Chinese Cyberwarfare*, William T. Hagestad II suggests: "The 'Middle Kingdom,' which is China, is determined, and in their focus destined to achieve worldwide leadership through the use of their state-sponsored, military-developed, and civilian-executed information dominance."[8]

As Hagestad does in his book, it is important to distinguish between the types of Chinese hackers, as their intentions and command and control structures vary. Most often associated with hacking U.S. computer networks, the PLA, under orders from the Communist Party of China (CPC), hacks as a means to equal the playing field between itself and the U.S. in the event of a crisis or war. China's cyberwarfare doctrine began to take shape after PLA officials saw the power that modern, information-enabled forces had during the Persian Gulf War. The U.S. targeted Iraqi command and control sites during the air campaign in order to disrupt its flow of information. U.S. armed forces were also able to use information to coordinate and synchronize movements and attacks. In an interview with PBS Frontline, John Arquilla, an associate professor at the Naval Postgraduate School, suggests that "the cyber things we did in the last Gulf War had much to do with the management of our own information."[9] Seeing how the U.S. used information dominance in the Gulf War, the PLA realized that in any hypothetical, future conflict with the U.S., achieving information dominance would be necessary in order to be victorious. To do so, the Chinese would need to use cyberattacks to disrupt U.S. command and control networks, effectively disrupting the flow of information and intelligence. Thus, as it stands today, the PLA's primary motive is "to map military capabilities that could be exploited during a crisis."[10]

In contrast, yet often in conjunction with the PLA, state-owned enterprises (SOE) use cyberwarfare for industrial espionage. As Hagestad notes, these SOEs are "successful multinational commercial enterprises, which must now compete on the world stage, without the benefit of knowing how to compete fairly."[11]

The industrial espionage typically associated with Chinese state-owned enterprises often concerns weapon designs and weapon systems.

The industrial espionage typically associated with Chinese SOEs often concerns weapon designs and weapon systems. While the PLA often benefits from having these designs, so do SOEs. For example, the Chinese J-31 fighter bears a remarkable resemblance to Lockheed Martin's F-35 Joint Strike Fighter. However, the PLA did not build the J-31; Shenyang Aircraft Corporation built it. Similarly, the J-20 fighter built by Chengdu Aircraft Industry Group closely resembles Lockheed Martin's F-22 Raptor. Interestingly, it has been suggested that Pentagon insiders question the Raptor's ability to perform in combat due to the extensive hacking that subcontractors faced while working on the fighter.[12]

Moreover, SOE-sponsored hacking is not limited to U.S. defense contractor weapon designs. SOE-sponsored hacking plays a role in China as well. For example, Edward Wong of *The New York Times* reported that Sany Group, a construction equipment manufacturer in China, used hackers to spy on a rival company, Zoomlion.[13] There are also political motivations for Chinese hacking. China's "Great Firewall" and Internet censorship have been well documented over the years. According to Wong, "local police departments contract

with companies like Xhunter to monitor and suppress dissent" within China itself.[14] Furthermore, he notes that Ai Weiwei, an artist who was arrested in 2011, stated that "every time anyone is arrested or checked, the first thing [the authorities] grab is the computer."[15] The CPC also uses information gathered by the PLA to map the decision-making process of policymakers and their professional networks, as suggested by the Pentagon's "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013." According to Brian Manzec, "The goal is not to deter other nations from conducting cyberwarfare against the People's Republic of China; rather, it is to use the threat of cyberwarfare to deter an actor from behaving in a manner that is in opposition to Chinese strategic interests."[16]

...hackers themselves often move between the government, military, and corporate positions looking for the largest paycheck.

While the various actors and interested parties engaged in hacking have been identified in China, it does not prevent overlap. As demonstrated, information gathered by the PLA is often used by SOEs or the CPC. Additionally, hackers themselves often move between the government, military, and corporate positions looking for the largest paycheck. Some are even outsourced. An anonymous hacker, quoted in *The New York Times*, adds some important insight on the monolithic nature of hacking in China. "China's government is so big. It's almost impossible not to have any crossover with the government….[The hackers] work for one thing, and that's for money."[17] Ultimately, while there are many interpretations of why the Chinese conduct cyberespionage campaigns, Hagestad's interpretation fits current, global affairs quite well since it makes note of the CPC's intentions on the global stage. "The motivation of the People's Republic of China to conduct cyberwarfare is comprised of fear, self-preservation, and hegemony."[18] One cyberattack, in particular, highlights how multiple Chinese parties benefited from hacking an American defense contractor.

A Bloomberg News investigation, using hacked HBGary Inc. emails from the hacking collective "Anonymous," found that QinetiQ North America was hacked over a three-year operation in which "most, if not all of the company's research" had been compromised by PLA Unit 61398.[19] While the investigation focuses solely on QinetiQ, it does make note that "QinetiQ was only one target in a broader cyberpillage," and that almost every defense contractor in the U.S. was a victim of Chinese cyberattacks during the same period.[20] This long-running hacking operation demonstrates that Chinese hackers have revolving targets that reflect different objectives.

Following the precedent of mapping U.S. networks, one focus of the QinetiQ operation was mapping shared networks between U.S. defense contractors, the government, and the military. For example, NASA alerted QinetiQ that one of its computers was used by hackers to try and infiltrate the agency's network.[21] Likewise, a cyber breach at the Redstone Arsenal, home of the Army's Aviation and Missile Command, Materiel Command, and the Missile Defense Agency, was also linked to a shared network with QinetiQ.[22] The attacks on these networks have allowed the PLA to map important shared networks between the military and defense contractors, not only to exploit during a war, but to also pilfer weapon systems' designs in order to exploit these systems in a war-time scenario or use the designs to manufacture their own.

According to this investigation, the Chinese hackers targeted specific engineers because they

were interested in "an innovative maintenance program for the Army's combat helicopter fleet."[23] Specifically, the target was the U.S. Army's Condition-Based Maintenance (CBM) program. This program was a cybertarget as on-board sensors collect data on deployed Army helicopters, which would allow the PLA to examine the deployment, performance, and maintenance needs of the Army's helicopter fleet.[24] According to an Army logistics presentation, the data gathered by these sensors includes classified command and control information, which gives the PLA access to valuable information, such as secure radio and identification friend or foe frequencies used by the Army. In another case, the hackers also targeted QinetiQ's advanced robotics unit. Not only did the Chinese use the stolen intellectual property to build a bomb disposal robot, similar to QinetiQ's "Dragon Runner," but it also allowed the PLA to understand the hardware the U.S. would deploy in a military conflict. Noel Sharkey, a robotics expert at Britain's Sheffield University, speaking to Bloomberg, suggested that the "chip architecture" used to build the PLA knock-off of the Dragon Runner could also be used against U.S. robotics or unmanned aerial vehicles.[25]

The cyberattack on QinetiQ also illustrates the need for defense contractors to plan for and execute cyberdefense plans. In the case of this hack, the company often ignored recommendations from advisors. "They felt like it was this limited little thing, like they'd picked up some virus," Brian Dykstra, a computer forensics expert said.[26] Worried about the costs associated with patching its networks, executives at QinetiQ continued to ignore recommendations by these hired advisors. In an interview, William Ribich concluded that QinetiQ was worried about the costs associated with securing its computer networks after the breach. A fix, recommended by Mandiant, was ignored. Consultants HBGary and Verizon Terremark faced similar challenges while trying to secure QinetiQ's networks. HBGary faced criticism from both Terremark and QinetiQ, and further believed Terremark was hoarding valuable data for itself. In another example, employees at QinetiQ would often delete security software installed by HBGary. As such, this cyber incident at QinetiQ was a perfect storm—a company with lax security, working on top secret military projects, met a formidable and malicious foe in Unit 61398. While fixes were recommended, they were often ignored by executives or resulted in backlash from employees. In the end, the Pentagon released a statement early in 2013 saying that the QinetiQ leaks were being probed. That statement would later be retracted by the Department of Defense, with spokesman Damian Pickart saying "while the reports of cyber intrusions against QinetiQ are disturbing, the Department of Defense is not in a position to investigate the security practices of a private company—including cleared defense contractors."[27] Overall, the attack on QinetiQ demonstrates the need for companies, in this case, defense contractors, to effectively secure their networks in order to guard valuable military information.

...the attack on QinetiQ demonstrates the need for companies, in this case, defense contractors, to effectively secure their networks in order to guard valuable military information.

According to Mandiant's report on Unit 61398, Chinese hackers begin their attacks on companies with a spear-phising campaign. In such a campaign, hackers send out emails with malicious files attached in hopes that an unsuspecting employee downloads the

attachment, opening a gateway into the target's network. Mandiant further suggests that "spear-phising is [Unit 61398]'s most commonly used technique."[28] In order to defend against such campaigns, defense contractors, including Lockheed Martin and Northrop Grumman, spear-phish their own employees to increase awareness of hackers' techniques to infiltrate computer networks.

According to reports, Northrop Grumman began spear-phising employees in 2009, and has "made running phising exercises a regular habit."[29] The goal of these exercises is to raise awareness among employees of such spear-phising campaigns, regardless of their origins. Brian Fung of the *National Journal* reported that a recent, internal campaign at Northrop Grumman targeted 68,000 employees using the façade of errors on their tax returns as a feint.[30] Similarly, Lockheed Martin began their "I Campaign" in 2009, which targets employees with spear-phising emails as well. These "messages are customized for various groups or individuals in the company" as the attack on QinetiQ often targeted groups of employees or individual business sectors, such as the company's robotics unit.[31] Both Lockheed Martin and Northrop Grumman have reported increased awareness and reporting of these attacks among employees. Chandra McMahon, Chief Information Security Officer (CISO) at Lockheed Martin claims, "I can say definitely that not only do I have more employees taking good actions with regard to emails, but more are reporting suspicious emails to the [Computer Incident Response Team]—and attacks have not been able to get started."[32] Similarly, Michael Papay, CISO for Northrop Grumman, makes a similar point. "If I've got 70,000 employees who are smart enough to say, 'Whoa, looks like a spear-phishing e-mail—I'm going to report it to my cybersecurity operations center,' then my operations center can dig into it and immediately block anyone else in the company from getting that e-mail."[33] Lockheed Martin has also launched products geared toward managing cybersecurity problems. In a 2010 interview with *National Defense Magazine*, the former director of the Defense Information Security Agency and Vice President of Cybersecurity Solutions for Lockheed Martin Charles Croom discussed that the company was automating software and using an encrypted thumb-drive, called "IronClad," to manage cybersecurity needs.[34] While these defense contractors and their competitors continue to work on improving their networks' security, they are also engaging hackers on the front lines of the cyberwar.

Aided by hackers, defense contractors, and the technology industry, U.S. defense and intelligence agencies have turned the world of security research upside down.

Speaking anonymously to Reuters, a former defense contractor executive was quoted as saying "my job was to have 25 zero-days on a USB stick, ready to go," referring to attacks which exploit unknown vulnerabilities in computer programs.[35] While the majority of media reports on Chinese cyberespionage, the offensive cyber capabilities of the U.S. are often overlooked, and for good reason, as "details about the U.S. offensive cyber capabilities and operations are almost all classified."[36] Aided by hackers, defense contractors, and the technology industry, U.S. defense and intelligence agencies have turned the world of security research upside down. In order to gather intelligence on foreign targets and exploit networked military systems, the National Security Agency has reportedly become the largest buyer of security exploits.[37] Companies such as Harris Corporation, Northrop Grumman, and Raytheon

have acquired boutique firms that focus on exploiting these vulnerabilities. Information on bugs in popular Microsoft software is given to U.S. intelligence agencies before the company releases a public patch to secure these flaws.[38] Furthermore, in hacked emails, leaked by Anonymous, the capabilities of Endgame Inc. were exposed as well. The company, chaired by the CEO of the Central Intelligence Agency's venture capital firm In-Q-Tel, markets zero-day exploits and the ability to mobilize and exploit criminal botnets in order to relay important information to clients, including intelligence agencies. However important cyberoffense is to maintaining intelligence capabilities or exploiting and degrading enemy networks, it also comes at a price, and according to Charlie Miller, a security researcher at social media giant Twitter, "the only people paying are on the offensive side."[39]

While these zero-day exploits are being used offensively, the Department of Homeland Security (DHS) has also set up a system to use them defensively, a move which will aid the defense of computer networks tremendously. Through the "Enhanced Cybersecurity Services" (ECS) program, information gathered by defense contractors, intelligence agencies, and telecommunications providers will be offered to other companies, notably those in the critical infrastructure and financial industries.[40] While this program takes a substantial step toward defending the nation's networks, it is important to note that the ECS program is young and still evolving. The ECS program has also come under fire for being too limited. Security officers laud the program for what sharing it does do, but also acknowledge that the government and chosen providers, such as Northrop Grumman and Raytheon, limit the shared data because these vulnerabilities have valuable, offensive capabilities. Wolfgang Kandek, Chief Technology Officer of Qualys states, "From an offensive point of view, it is certainly valuable to maintain a certain number of exploits in private, but for defense the best option is to share the vulnerability information with the software vendor as quickly as possible."[41] Echoing this sentiment, research director for NSS Labs Andrew Braunberg critiques the ECS program stating, "Most obviously, the U.S. government wants it both ways. They don't really want these vulnerabilities to disappear because they want to use them offensively, but they don't want the same vulnerabilities to allow hacking of U.S. assets."[42]

While the ECS program takes an important step in sharing information on network vulnerabilities with companies in the U.S. that could be exploited by Chinese hackers, revelations of the National Security Agency's domestic intelligence gathering could cause a backlash among Americans that harm further efforts to scan Internet traffic aimed at protecting networks from hackers. Under the ECS program, Web traffic that flows into and out of private businesses will be scanned for irregularities, which was initially limited to defense contractors and government agencies. Yet, as revelations about the National Security Agency's PRISM program were leaked to the press by Edward Snowden, more Americans have become aware that information transmitted online was being scanned and could increasingly be scanned as the government seeks to limit cyberattacks. These concerns

...as revelations about the National Security Agency's PRISM program were leaked to the press by Edward Snowden, more Americans have become aware that information transmitted online was being scanned...

could be further echoed by legislators as the debate on the Cyber Intelligence Sharing Protection Act faces Congressional scrutiny, since the legislation seeks to share more threat intelligence with the National Security Agency. Absent and fractured leadership on cybersecurity also threatens the defense of America's computer networks.

Faced with securing civilian networks and assisting the private sector, DHS faces a void of leadership that could complicate efforts to protect American networks from hackers. While these leadership roles can be filled, these vacancies represent a larger, troubling trend for the department as it must compete for hackers and qualified professionals with the National Security Agency and private industry. In an effort to attract technology students to government service, the National Science Foundation's CyberCorps Scholarship for Service program saw a majority of its graduates go on to work for the National Security Agency instead of DHS.[43] Furthermore, on average, government salaries fail to match those offered in industry. For instance, a cybersecurity professional working in government makes $99,000, while the average in industry is $107,000. While the DHS and government as a whole struggle with these discrepancies, Dr. Daniel Goure, vice president of the Lexington Institute, believes this is actually a positive trend. Following the release of the Defense Science Board's report, he penned an opinion piece that called on the private sector to defend the nation's networks, as many defense contractors have set up cybersecurity units in order to plug their leaks. "Major defense companies such as Lockheed Martin, Boeing, Northrop Grumman, and General Dynamics stood up cyberdefense units, initially to protect their own networks and computer systems. In many ways, these companies are now on the front line of the ongoing and intensifying cyberwar."[44] Goure also points out that as private companies, defense contractors have a particular interest in defending their networks and creating cost-effective cybersecurity solutions to market to government agencies and other businesses. He concludes by stating that "when it comes to cyberdefense, the nation increasingly is dependent on the private sector."[45] Goure's statement is echoed by both Boeing and Lockheed Martin who provide their expertise in cybersecurity to their clients.[46] Boeing markets its cybersecurity capabilities commercially using the solutions they employ in-house as the product. Using this technique allows Boeing "to sell that one product many times," according to Bryan J. Palma, vice president of security and information services for Boeing.[47]

This private sector-led model for cyberdefense may be a good fit for U.S. government agencies. As China's CPC uses the PLA and outsourced hackers from SOEs and skilled individuals, the private sector-led model could provide cyberdefense to U.S. government agencies and critical infrastructure. The U.S. government's role in cyberdefense and cyberoffense must be greater. Placing the Homeland Security and Defense departments in regulatory and oversight roles will allow the government to set guidelines and standards that these private sector companies must follow in securing U.S. cyber vulnerabilities. This will also create competition for commercial and government contracts that will continue to drive innovation in cybersecurity research. Potentially, these private sector contactors may also be able to use threat intelligence and intelligence gained by hacking back through intelligence agencies to infiltrate and map Chinese networks for the Department of Defense. However, it would be the role of U.S. government agencies to set limits on the contractors' offensive measures, preventing future conflicts or a full-blown cyberwar. ***IAJ***

NOTES

1 Emil Protalinski, "NSA: Cyber Crime is 'the Greatest Transfer of Wealth in History,'" ZDNet homepage, U.S. edition, <http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598>, July 10, 2012, accessed on June 4, 2013.

2 Richard Koman, "Estonia Reeling from Massive Cyberattack from Russia," ZDNet homepage, U.S. edition, <http://www.zdnet.com/blog/government/estonia-reeling-from-massive-cyberattack-from-russia/3161>, May 18, 2007, accessed on June 4, 2013.

3 Ellen Nakashima, "U.S. and Russia Sign Pact to Create Communication Link on Cybersecurity," *The Washington Post* homepage, <http://articles.washingtonpost.com/2013-06-17/world/40025979_1_cyber-security-pact-homeland-security>, June 17, 2013, accessed on June 18, 2013.

4 Verizon RISK Team, "2013 Data Breach Investigations Report," <www.verizonenterprise .com/DBIR/2013/>, accessed on March 25, 2013.

5 Bill Gertz, "Network Effects: Chinese University Linked to PLA Cyber Attacks," Free Beacon homepage, < http://freebeacon.com/?s=Network+Effects&submit=>, May 14, 2013, accessed on May 15, 2013.

6 Cadie Thompson, Businesses Consider Going Offense Against Cyberattackers," CNBC homepage, <http://www.cnbc.com/id/100789013>, June 4, 2013, accessed on June 8, 2013.

7 Edward Wong, "Hackers Find China is Land of Opportunity," *The New York Times* homepage, <www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html>, May 22, 2013, accessed on May 23, 2013.

8 William T. Hagestad II, *21st Century Chinese Cyberwarfare*, IT Governance Publishing, Cambridgeshire, UK, 2012, p. 2.

9 PBS Frontline, Interview: John Arquilla, Frontline homepage, <http://www.pbs.org

/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>, March 4, 2003, accessed on May 27, 2013.

10 David E. Sanger, "U.S. blames China's Military Directly for Cyberattacks," *The New York Times* homepage, <http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html>, May 6, 2013, accessed on May 7, 2013.

11 Hagestad, p. 5.

12 Michael Riley and Ben Elgin, "China's Cyberspies Outwit Model for Bond's Q," Bloomberg homepage, <http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html>, May 2, 2013, accessed on May 2, 2013.

13 Wong.

14 Ibid.

15 Ibid.

16 Hagestad, p. 33.

17 Wong.

18 Hagestad, p. 26.

19 Riley and Elgin.

20 Ibid.

21 Ibid.

22 Ibid.

23 Ibid.

24 Ibid.

25 Ibid.

26 Ibid.

27 Ben Elgin, "Pentagon Retracts Statement on Probe of QinetiQ Hacking," Bloomberg homepage, <http://www.bloomberg.com/news/2013-05-07/pentagon-retracts-statement-on-probe-of-qinetiq-hacking.html>, May 7, 2013, accessed on May 8, 2013.

28 "APT1: Exposing One of China's Cyberespionage Units," Mandiant Intelligence Center, <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>, p. 28, accessed on March 5, 2013.

29 Brian Fung, "This Defense Contractor is Reportedly Spear-Phising 68,000 Innocent People," *National Journal* homepage, <http://www.nationaljournal.com/tech/this-defense-contractor-is-repeatedly-spear-phishing-68-000-innocent-people-20130403>, April 3, 2013, accessed on April 4, 2013.

30 Ibid.

31 Kelly Jackson Higgins, "How Lockheed Martin Phishes Its Own," InformationWeek: Dark Reading homepage, <http://www.darkreading.com/risk/how-lockheed-martin-phishes-its-own/d/d-id/1139629>, April 25, 2013, accessed on April 28, 2013.

32 Ibid.

33 Fung.

34 Sandra I. Erwin, "Surge of Cybersecurity Bureaucracies Sparks Lucrative Opportunities for Industry," National Defense homepage, <http://www.nationaldefensemagazine.org/archive/2010 /September/Pages/SurgeofCybersecurityBureaucraciesSparksLucrativeOpportunitiesForIndustry.aspx>, September 1, 2010, accessed on May 30, 2013.

35 Joseph Menn, "Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback," Reuters homepage, <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510?, May 10, 2013, accessed on May 15, 2013.

36 Warren Strobel and Deborah Charles, "With Troops and Techies, U.S. Prepares for Cyber Warfare," Reuters homepage, <http://www.reuters.com/article/2013/06/07/us-usa-cyberwar-idUSBRE95608D20130607>, June 7, 2013, accessed on June 12, 2013.

37 Menn, "Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback."

38 Michael Riley, "U.S. Agencies Said to Swap Data with Thousands of Firms," Bloomberg homepage, <http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.

html>, June 14, 2013, accessed on June 16, 2013.

39 Menn, "Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback."

40 Joseph Menn, "U.S. to Protect Private Sector from Secret Software Attacks," Reuters homepage, <http://www.reuters.com/article/2013/05/15/us-cyber-summit-flaws-idUSBRE94E11B20130515>, May 15, 2013, accessed on May 15, 2013.

41 Antone Gonsalves, "Experts Ding DHS Vulnerability Sharing Plan as Too Limited," CSO homepage, <http://www.csoonline.com/article/733557/experts-ding-dhs-vulnerability-sharing-plan-as-too-limited>, May 17, 2013, accessed on May 20, 2013.

42 Ibid.

43 Nicole Perlroth, "Tough Times at Homeland Security," *The New York Times*, Bits section homepage, <http://bits.blogs.nytimes.com/2013/05/13/tough-times-at-homeland-security>, May 13, 2013, accessed on May 14, 2013.

44 Daniel Goure, "U.S. Defense Contractors Have Developed Serious Cybersecurity Capabilities," Lexington Institute homepage, <http://www.lexingtoninstitute.org/us-defense-companies-have-developed-serious-cyber-security-capabilities?a=1&c=1171>, May 29, 2013, accessed on May 29, 2013.

45 Ibid.

46 Marjorie Censer, "Defense Contractors Translate Their Own Cybersecurity Protections into Business," *The Washington Post*, Capital Business section homepage, <http://www.washingtonpost.com/business/capitalbusiness/defense-contractors-translate-their-own-cybersecurity-protections-into-business/2013/03/17/75e7098c-82a6-11e2-b99e-6baf4ebe42df_story.html>, March 17, 2013, accessed on March 25, 2013.

47 Ibid.