Security issues of contractors in the american military

Abstract

This paper will show examples of how the United States military has become over-dependent on the use of government contractors. The military cannot fight a war, or create new weapons technology, or maintain its current weapons without the use of contractors. Some of these contractors are given access to classified information, occasionally at the highest levels. National state actors have been attacking our cleared defense contractors' networks in order to gain access and information to sensitive military networks and weapon systems. Nation state actors have been ex-filtrating information on a large scale from these networks, which gives away our military's technological advances to other entities. I will discuss how these attacks have been happening, what has been stolen, and how the United States Government is regulating the protection of vital military information.

Contractors: An American Military Weakness?

Contractors are used by the United States' military organizations to complete research and development, weapon system management, security, or day-to-day positions to supplement uniformed personnel. The United States military decided to hire more contractors to work in support roles such as food services, maintaining housing, water purification, and others in the 1980s (Weisgerber, 2016). The government has become even more dependent on the use of contractors to fill gaps that government personnel can no longer fill. The use of contractors within the Department of Defense has boomed overseas and at home with the wars in Afghanistan and Iraq and a limited amount of uniformed military personnel. During World War II,

about 10 percent of the armed forces were contracted (McFate, 2016). According to the Commission on Wartime Contracting in Iraq and Afghanistan, the Department of Defense had 207, 553 contractors employed in Iraq and Afghanistan in March 2010, generally matching one-to-one with military members deployed, or 50 percent (2011). As of 2016, the rise of contractor utilization in Afghanistan had ballooned to 75 percent of all personnel located throughout the country.

Contractors do not count as troop-strength within the Department of Defense. In 2016, the maximum allowed military members allowed in Iraq was capped at 4, 647 troops, so to fill the void, another 4, 970 contractors were deployed to Iraq to assist with the mission (Ong, 2018).

During fiscal year 2014, 8 percent of all federal spending, or $285 billion, were obligated to federal contracts (McFate, 2016). In perspective, the Pentagon three and a half times more than Great Britain’s entire defense budget on contracting. The American military can no longer conduct war without the private sector.

With the dependence of contractors within the Department of Defense, contractor facilities are getting access to classified networks within their facilities. However, some of the organizations’ cybersecurity protections are lacking, allowing nation-state actors and other hackers access to sensitive or classified information, without attacking the military networks directly.

The Defense Security Service determines the eligibility of contractors to access classified information, including facilities. Once cleared, using periodic security reviews, the Defense Security Service is responsible for

ensuring that the contractors meet the requirements to safeguard classified information. The Defense Security Service is also tasked to investigate if defense contractor organizations have any foreign influence or ownership as a condition of access. The Defense Security Service depends on the contractor to self-report information that could have a foreign influence or ownership. As of June 2017, approximately 630 of the 12, 000 cleared facilities had a migration agreement to address foreign influence or ownership concerns (Government Accountability Office, 2018).

The National Industrial Security Program Operating Manual states that a contractor, or prospective contractor, is eligible for a facility clearance if there is a valid need for access to classified information in connection with a legitimate United States Government contracting requirement.

In the Government Accountability Office Report 18-407, the Defense Security Service notified Congress that they were unable to conduct security reviews at 60 percent of cleared defense contractors in Fiscal Year 2016 (2018). The Defense Security Service stated that each field office averaged 8 industrial security personnel overseeing about 470 facilities. In addition, with this heavy workload, industrial security personnel might be able to respond quickly to threats at cleared facilities. The workload won’t get any easier as the National Defense Authorization Act of Fiscal Year 2018 directed the Defense Security Service to reassume background and security investigations for all Department of Defense personnel, not just contractors.

The Defense Security Service announced in 2017 that the United States was facing the most significant foreign intelligence threat that it had ever

encountered and adversaries were attacking cleared facilities at unprecedented rates. To combat this ever-changing landscape, the Defense Security Service is creating a program to prioritize the facility reviews to align with the Department of Defense's list of critical technologies and programs called DSS in Transition. According to the Government Accountability Office, the amount of resources or additional personnel required for this new program has not been identified.

Breach After Breach

The Government Accountability Office warned in 1996 that hackers had taken control of whole defense systems. In 2004, warnings of the Pentagon's intent on connecting more systems through the Internet would provide more opportunity for hackers to gain access.

On July 14, 2011 during a speech at the National Defense University in Washington D. C., William Lynn, the Deputy Secretary of Defense, had admitted that a foreign government was behind a major data breach from a defense contractor in March of 2011 where 24, 000 files were taken (Department of Defense, 2011). Deputy Lynn stated, " In looking at the current landscape of malicious activity, the most prevalent cyber threat to date has been exploitation or the theft of information and intellectual property from government and commercial networks." During his speech, Deputy Lynn mentioned that terabytes of data had been extracted from corporate networks of defense companies from foreign intruders. Data exfiltrated from the defense contractors included specifications from small parts of tanks, airplanes, submarines, aircraft avionics, surveillance

technologies, satellite communications systems, missile tracking systems, and the Joint Strike Fighter. The exfiltration of this sensitive data has not been stopped by current countermeasures.

In a 2013 public report by the Defense Science Board, the advisory group claimed that the Pentagon was unprepared to counter a full-scale cyber-conflict (Nakashima, 2013). The same report warned that the electronic intrusions of advanced technologies can accelerate the development of Chinese weapons systems and weaken United States military advantages in future conflicts. With the information included in these intrusions, other governments could create new weapons similar to American weapons, or could use the information to find flaws in our weapons and exploit them. The information regarding the ballistic-missile defense systems could show the range and detection signature types for identifying projectiles from other countries and create a new missile not identified via the specifications stolen. The theft of information saves billions of dollars in development costs of advanced technologies

The costliest data theft through contractor networks is the F-35 Lightning II Joint Strike Fighter. The Pentagon’s $300 billion project to create the most technologically-advanced stealth fighter jet was believed to be stolen by Chinese hackers. The jet that is created by Lockheed Martin Corporation, Northrop Grumman Corporation, and BAE Systems depend on 7. 5 million lines of code to operate. The data was stolen by compromising the system that diagnoses maintenance problems during flight. The systems were infected through two of the three contractor networks connected to the Internet as early as 2007. The spies had inserted technology that encrypts

the data as it’s being stolen, therefore investigators couldn’t identify what specifically had been stolen (Gorman, Cole, & Dreazen, 2009).

Five years after the theft of the Joint Strike Fighter program data, the Chinese military made its first appearance of its J-31 stealth fighter, an almost exact replica of the F-35 Joint Strike Fighter (Brown, 2018). While the Chinese government denied stealing the data and blaming the United States of Cold War tactics, no believed that the Chinese could create a replica of the jet without the data. The data spies were unable to get classified information on the jet, so while the physical design was nearly identical, some flight sensors and other flight systems were not replicated. The Chinese jet weighs roughly the same, but has a lower maximum takeoff weight by 14, 000 pounds and can only fly about half the range as the American’s jet, therefore not an exact replica.

United States officials stated that a Navy Contractor working for the Naval Undersea Warfare Center in Newport, Rhode Island was compromised by Chinese hackers in January and February 2018 (Nakashima & Sonne, 2018). The hackers for the Chinese government stole 614 gigabytes of material relating to signals and sensor data, the Navy submarine development unit’s electronic warfare library, submarine radio room information relating to cryptographic systems, and a highly sensitive project called Sea Dragon, of which the Pentagon has already spent $300 million on. Sea Dragon tasked to develop a supersonic anti-ship missile for use on submarines by 2020. The information for this project was located on the contractor’s unclassified network, however, when the material was compiled together, the information could be considered classified. Department of Defense Secretary Jim Mattis

had asked the Pentagon’s Inspector General Office to review contractor cybersecurity issues after news of the incident were reported. According to the Navy, details on hundreds of mechanical and software systems were compromised.

In September 2015, an agreement between President Barack Obama and Chinese President Xi Jinping was signed stating that China would cease conducting commercial espionage against the United States’ corporations. The one-sided agreement was signed by the Chinese in an effort to avoid economic sanctions from the United States. While it appears that data theft had slowed from China, it did not stop all together.

The agreement does not prevent spying on military technology specifically. “ The distinction we’ve always made is there’s a difference between conducting espionage in order to protect national security and conduct military operations, and the theft of intellectual property for the benefit of companies inside your country,” said Michael Daniel, the White House cybersecurity coordinator under Obama (Nakashima & Sonne, 2018).

According to Director of National Intelligence, Daniel Coates, “ China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities” (2018, p. 6). Director Coates continues to summarize that cleared defense contractors whose products and services support government networks worldwide that are most detected are Chinese cyber operations, most likely from the newly created Strategic Support Force in 2015.

The cyber espionage doesn’t just occur against the United States. The largest Japanese defense contractors Mitsubishi Heavy Industries and IHI were victims of a cyberattack. On August 11, 2011, eight different types of malware were discovered on 45 servers and 38 computers (Kallender-Umezu, 2011). This is a concern for United States military personnel because Mitsubishi Heavy Industries creates parts for Lockheed Martin and Raytheon in missile technologies, space launch vehicles, and F-15 fighter jets used by the government.

Due to the global nature of contracting and supply chain management, the Risk Management Framework has a family of security controls that assess and validate system’s supply chains. Program offices and contract entities must be able to document the entire chain of products and services from cradle to grave on where they are made and who had access during the production process. As evidenced through the Japanese cleared defense contractors breach, the production process was infected along the way, and could have been passed on to the United States Government networks if not accounted for along the way. These security controls are heavily dependent on documentation, similar to a chain of evidence in a criminal trial; every entity that touches the products needs to be documented, or the process cannot be trusted as secure.

Supply chain management security can cause issues for software makers as well. CCleaner, a software used to digitally clean computers of potential malware, was found to have malicious code to steal customer’s data added to its software during the production process as identified by Cisco Talos (Simon, 2017). Avast, the corporation that owned CCleaner, was unaware

the software was infected, and millions of customers had received the malicious product. Luckily, the identification of the tainted software was made days after it was publicly available, but it still caused problems for an unknown number of users.

While this research paper details some of the publicly known breaches, President Trump's administration is expected to declassify intelligence relating to the campaign of cyber intrusions, dating back to 2014, in an effort to indict government hackers assigned to China's Ministry of State Security (Stark, 2018).

According to government security audits from 2012 to 2017, almost all weapon systems in the United States military suffer from mission-critical cyber vulnerabilities (Gregg, 2018). The Government Accountability Office released a report regarding cybersecurity of weapon systems that utilized security audits of skilled testers. These testers were able to easily attack nearly every system. From basic security flaws of not changing the default passwords of operating systems, to guessing administrator passwords, to changing display messages and the ability to delete data. The report also stated that the found flaws on represent a fraction of the holes in the networks. The testers had a limited amount of time on the networks, therefore using only the most common or time-efficient vulnerabilities to gain access.

The report from the Government Accountability Office noted that program officials failed to correct 19 of 20 cyber-vulnerabilities that were previously assessed stating contractor errors were to blame (Gregg, 2018). This shows

a lack of oversight and responsibility on behalf of the government, resulting in a lack of confidence in our weapons platforms.

Cybersecurity Becomes a National Priority

Due to the amount of cybersecurity attacks of contractor networks, new regulations were being drafted beginning in 2013, intended to protect unclassified controlled technical information, also known as covered defense information. Classified information already has rules and regulations on protection of the data, but there wasn't official parameters for protecting sensitive unclassified information. In 2016, Revision 1 of the National Institute of Standards and Technology (NIST) Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* , was published. The implementation of this regulation brings Risk Management Framework attributes to the contractor's networks, including the requirement to furnish the Government with a System Security Plan and any associated Plan of Action and Milestones (POAM) (Cassidy, 2016).

The Department of Defense issued an immediately-effective rule requiring contracts to include a clause imposing safeguarding and cyber-incident reporting obligations on information systems that process, store, or transmit covered defense information in October 2016.

Also in October 2016, the Department of Defense issued another final rule implementing mandatory cyber incident reporting requirements for all agreements with contractor and subcontractors. The rule announcement

also encouraged contractors to participate in the voluntary Defense Industrial Base cybersecurity information sharing program.

The Defense Industrial Base information sharing program a voluntary program where civilian companies alert the Department of Defense to attacks in their system and the military sends reports regarding the new threats to all participants in the program so they could see if they are targeted as well (Magnuson, 2013). The program is set up in a way that some classified information regarding cyber attacks and threats could be sent to the participants within the program, but only if they are cleared to the appropriate security clearance. The Defense Industrial Base program according to William Lynn, the Deputy Secretary of Defense in 2011 stated the government will not be monitoring, storing, or intercepting any private-sector communications (Department of Defense, 2011).

Section 1647 of the National Defense Authorization Act (NDAA) of Fiscal Year 2017 required:

The Secretary of Defense to establish an advisory committee to make recommendations for the protection of information and networking systems of cleared defense contractors, including information security and cyber defense policies, practices, and reporting relating to the unclassified information and networking systems of defense contractors. The advisory committee will be composed of six to ten members appointed by the Secretary of Defense, split between Government and industry representatives (Cassidy, 2017).

Another requirement of the National Defense Authorization Act of 2017 required the Secretary of Defense to report to Congress and the President on how to deter cyber-attacks by foreign governments via military and non-military options.

International law firm Covington & Burling's co-chair Robert Nichols said, " contractors of every size are being impacted by escalating regulatory requirements, and most contractors lack a robust cybersecurity program" (Sugarman, 2014). Startups companies usually cannot afford the compliance costs, which makes them the most vulnerable. Newer regulations may also require contractors to provide cybersecurity safeguards to their subcontractors, which increases the bottom line for the companies, causing them to take more risks.

Not all professionals believe the new regulations are required. Scott Phillpot, director of Cyber Protection Resources in Hampton Roads, Virginia, said, " It's just this unending march of cybersecurity overreach" (Pierceall, 2017). Phillpot estimates the new regulations will cost contracting corporations $500 to $1, 000 per employee per month to stay compliant, equating it to a tax to do government business.

The adversary will continue to change their attack tactics to gain information to American sensitive information. With the government sharing more threat data to defense contractors, the Chinese have begun attacking sub-contractors networks to gain information.

Major government defense contractors Northrop Grumman and Lockheed Martin have acknowledged that they are experiencing greater number of

attempts to penetrate the network. In addition, attacks on their supply chain partners are on the rise. The best news is that threat detection and reporting of cyber incidents has gotten must more robust and identified faster than the earlier days of the Internet.

No one can keep attackers out of their networks forever. With enough time and resources, a dedicated hacker can gain access to a network. When the hacker is paid to hack networks, the attacks can be methodical and slow, reducing the chances of getting caught in a timely manner.

Government contractors don’t take an oath to our country like military personnel during enlistment. Contractors are not bound by the Uniformed Code of Military Justice either. A government contractor can get up and quit their job whenever they like, unlike military personnel. The use of contractors within the military is similar to mercenaries; hired hands and guns to do the jobs others can’t or don’t want to do. In the end, the contractor is interested in the money. Within my military organization, anytime the unit requests assistance from our cleared defense contractor, the contractor needs to ensure it is within the scope of the contract and the government has money allotted to satisfy the request already. If not, a contract modification needs to be completed, and since they are the prime contractor, tend to charge more knowing that the action needs to be completed.

References

- Cassidy, S. B. (2017, February 10). DoD Further Clarifies Its DFARS Cybersecurity Requirements. Retrieved December 8, 2018, from

https://www. insidegovernmentcontracts. com/2017/02/dod-clarifies-dfars-cybersecurity-requirements/

- Coates, D. R. (2018, February 13). Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community. Retrieved December 9, 2018, from https://www. dni. gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI. pdf
- Commission on Wartime Contracting in Iraq and Afghanistan. (2011, August). Transforming Wartime Contracting: Controlling costs, reducing risks. Retrieved December 13, 2018, from https://cybercemetery. unt. edu/archive/cwc/20110929213815/http://www. wartimecontracting. gov/
- Department of Defense. (2011, July 14). Remarks on the Department of Defense Cyber Strategy. Retrieved December 12, 2018, from http://archive. defense. gov/speeches/speech. aspx? speechid= 1593
- Gorman, S., Cole, A., & Dreazen, Y. (2009, Apr 21). Computer spies breach fighter-jet project. Wall Street Journal Retrieved from http://library3. webster. edu/login? url= https://search-proquest-com. library3. webster. edu/docview/399049626? accountid= 14944
- Government Accountability Office. (2018, May 14). Protecting Classified Information: Defense Security Service Should Address Challenges as New Approach Is Piloted. Retrieved December 6, 2018, from https://www. gao. gov/products/GAO-18-407
- Gregg, A. (2018, October 14). Defense industry grapples with cybersecurity flaws in new weapons systems. Retrieved December 9, 2018, from https://www. washingtonpost.

com/business/economy/defense-industry-grapples-with-cybersecurity-flaws-in-new-weapons-systems/2018/10/14/b1de3bae-ce36-11e8-a360-85875bac0b1f_story. html? noredirect= on&utm_term=. 0ce490660b7b

- Kallender-Umezu, P. (2011). Cyber Attackers Strike 2 Major Japanese Defense Contractors. Defense News, 26(35), 4–8. Retrieved from https://library3. webster. edu/login? url= https://search. ebscohost. com/login. aspx? direct= true&db= mth&AN= 66756911&site= ehost-live
- Magnuson, S. (2013). Cybersecurity Executive Order Can Only Do So Much; New Legislation Needed, Official Says. National Defense, 97(713), 12. Retrieved from https://library3. webster. edu/login? url= https://search. ebscohost. com/login. aspx? direct= true&db= mth&AN= 91689984&site= ehost-live
- Nakashima, E. (2013, May 27). Confidential report lists U. S. weapons system designs compromised by Chinese cyberspies. Retrieved December 9, 2018, from https://www. washingtonpost. com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story. html? utm_term=. 08d6ae0de59a
- Nakashima, E., & Sonne, P. (2018, June 08). China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. Retrieved December 11, 2018, from https://www. washingtonpost. com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-

warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html? utm_term=. 0915d07da172

- Ong, D. (2018, November 27). Making A Killing. Retrieved December 11, 2018, from https://www. carolinapoliticalreview. org/editorial-content/2018/11/27/making-a-killing
- Pierceall, K. (2017, March 17). Military demanding all defense contractors keep up pace on cybersecurity. Retrieved December 8, 2018, from https://pilotonline. com/business/defense-shipyards/article_63edb03a-9643-5a1a-997b-899da000a3ef. html
- Stark, T. (2018, December 12). Morning Cybersecurity. Retrieved December 12, 2018, from https://www. politico. com/newsletters/morning-cybersecurity
- Sugarman, E. (2014, August 26). Cybersecurity Is A Severe And Growing Challenge For Government Contractors. Retrieved December 8, 2018, from https://www. forbes. com/sites/elisugarman/2014/08/26/cybersecurity-is-a-severe-and-growing-challenge-for-government-contractors/#12f61c82728e
- Simon, M. (2017). CCleaner hacked with malware: What you need to know. PCWorld, 35(11), 14–16. Retrieved from https://library3. webster. edu/login? url= https://search. ebscohost. com/login. aspx? direct= true&db= bth&AN= 125951730&site= ehost-live
- Weisgerber, M. (2016, February 23). Back to Iraq: US Military Contractors Return In Droves. Retrieved December 12, 2018, from https://www. defenseone. com/threats/2016/02/back-iraq-us-military-contractors-return-droves/126095/