Proceedings of the National Conference
On Undergraduate Research (NCUR) 2016
University of North Carolina Asheville
Asheville, North Carolina
April 7-9, 2016

Defending Against Cyber Espionage: The US Office of Personnel Management Hack as a Case Study in Information Assurance

Sarah Harvey and Diana Evans
Intelligence and National Security
Coastal Carolina University
100 Chanticleer Dr. E
Conway, SC 29528

Faculty Advisor: Dr. Joseph Fitsanakis

Abstract

In April 2015, the United States Office of Personnel Management (OPM) suffered the most extensive digital theft of government data in history, with a cyber hack that resulted in the loss of 21.5 million personnel records. Those affected included virtually all applicants for background checks since 2000. The scale of this breach has potentially catastrophic consequences for American national security, with some reports suggesting that US intelligence personnel has already been recalled from Beijing due to safety risks. The OPM hack reawakened the debate on how to better secure government data and limit potential damage to US national security. In broad terms, the US has the option to take defensive countermeasures as a form of protection, or offensive countermeasures as a form of deterrence. Defensive strategies center on allocating energy and resources to securing vulnerable systems. In contrast, offensive tactics involve economic sanctions, legal indictments, diplomatic protests, and offensive cyber operations of a pre-emptive nature. The Obama Administration is currently trying to determine the most effective route to retaliate against the primary suspect —China— without escalating an already tense bilateral relationship into an all-out cyber war. This paper outlines the US government's options in strengthening the protection of classified information. Specifically, should Washington adopt a defensive stance, or opt for an offensive response to cyber threats? To answer this question, this paper will examine the OPM hack case study under the prism of Information Assurance (IA), defined as the overall approach to identifying, understanding, and managing the risks to information systems. Based on the above methodology, this paper will argue that improving defensive security measures through the expansion of IA operations is prudent for two reasons: firstly, because they have a higher potential of actually securing classified information; and secondly, because they are less likely to jeopardize America's delicate relationship with China.

Keywords: Cybersecurity, Information Assurance, Office of Personnel Management

1. Introduction

In a realm such as cyber security, which has yet to establish guidelines, the response to cyber-attacks is inherently problematic. A recent breach in the United States OPM information systems resulted in the theft of millions of personnel files. Specifically, 21.5 million records are believed to have been compromised. The OPM released an official statement that elaborated: "Of the 21.5 million individuals whose Social Security Numbers and other sensitive information were impacted by the breach, the subset of individuals whose fingerprints have been stolen has increased from a total of approximately 1.1 million to approximately 5.6 million."[1] Information stolen includes, but is not limited to, passwords, credit cards, and Social Security numbers, which can be changed to prevent identity theft or fraud. However, fingerprints cannot. Although identity theft and fraud are highly unlikely in regard to the biometric information, the OPM did not rule out future problems as technology advances. Other recent hacks, such as those that occurred in RSA Security, Booz Allen Hamilton, and the International Monetary Fund, prove that cyber attacks are

becoming more frequent.[2] In regard to the OPM, the United States has abstained from any known retaliation towards the alleged perpetrator, China. It remains unclear whether the Chinese government or nonstate actors are responsible. Shortly before a state visit in September 2015 by President Xi Jinping, the Chinese government arrested a handful of hackers that it said were responsible for the OPM data breach. US officials speculate that arrests were an attempt by Beijing to lessen tensions with Washington.

2. Explanations and Definitions Concepts

Cyber espionage has been seen as an increasing threat to the national security of the US, a country with an ever-growing presence in the global military and political communications system, which today combines over 15,000 networks using 7 billion computing devices over hundreds of countries. The cyber realm is now being recognized as the new domain for warfare, alongside air, land and sea, as illustrated by the rapid rise in the frequency of attacks on computer networks over the past decade.[3] In addition to domestic IA strategies that are based on continuous monitoring, adversaries also unremittingly monitor for flaws and weaknesses within computer networks to exploit classified information that could potentially result in catastrophic damage. Possible targets include a nation's logistics network, domestic infrastructure systems such as water, electricity, and transportation, the financial system, as well as military facilities, weapons systems and databases.

Typically, the US defends against such attacks using either offensive or defensive approaches. Since October 2010, a new sub-unified command, named US Cyber Command (USCYBERCOM) has been fully operational, taking on the mission of both offensive and defensive cyber operations. The latter involve "planning, coordinating, integrating, synchronizing and conducting activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to [...] adversaries." [4]

One recent known penetration of the American cyber realm was in April 2015, against the US OPM. This office "works in several broad categories to recruit, retain and honor a world-class workforce for the American people."[5] Some of their responsibilities include: managing federal job postings, conducting security clearances and background investigations for potential employees, assuring the federal workforce upholds the merit system, and managing pension benefits for retired federal employees. Inevitably, the OPM is accountable for the storage of mass amounts of information, which in turn provides a target for adversaries looking to make a heavy impact with a single hack.

Information Assurance, closely related to the field of computer science and cybersecurity, aims to develop and implement effective computer security and risk management strategies to limit the unauthorized access to data within an information system, better known as a hack. IA experts strive to defend and protect information systems by relying on the proper application of the following concepts: confidentiality, integrity, availability, authentication, and non-repudiation. These five main qualities work together to protect information systems (IS). The first three elements, confidentiality, integrity, and availability, are referred to as the CIA Triad. The addition of authentication and non-repudiation comprises the five basic services described in the Maconachy-Schou-Ragsdale (MSR) model of IA. The MSR Model is an extension of the McCumber INFOSEC Model coined in 1991 by John McCumber.[6] The first element, confidentiality, is the assurance of data secrecy where no party is able to read the data except the intended entity.

A typical example of applying confidentiality is the compartmental classification system used in the military to label levels of secrecy, which an actor must possess in order to gain access. Secondly, integrity ensures that the data has not been altered by unauthorized individuals or processes. Application of a mathematical technique, which later will verify the information, is one example of achieving integrity. Availability, considered one of the most marketable properties of an IS, assures that information is available for use by those who need it, and blocks access to those who are deemed unauthorized. The term authentication can be used as a blanket term for the entire Identification, Authentication, Authorization, and Accountability (IAAA) process. Broadly, the function involves confirming that users are who they portray to be. Common methods for authentication are passwords, usernames, and biometrics. The final aspect to IA is non-repudiation, summarized as the inability to deny an action. Moreover, there is typically a record kept of when, where and who accessed certain information. All of these aspects combine to ensure the protection of the cyber domain.[7]

3. Argument

Even though most of the personal data stolen from the OPM hack, such as social security numbers, passwords, and credit cards, can be changed, other information, defined as permanent, cannot. Permanent information includes detailed background data, family details, and most importantly, biometric data such as fingerprints. Major consequences can result from the OPM hack, which resulted in the compromise of 21.5 million records belonging federal employees, job applicants and contractors. The ability to misuse biometric information may be limited; however the possible courses of illicit action pose major perils for the security of US government personnel. Assuming that China is behind the breach, which appears to be the tacit consensus in the relevant literature, it is plausible to suggest that the Chinese state has built databases of US government personnel, some of which is operational within China or specializes on Chinese affairs.[8] This database may contain the stolen biometric information, to red flag US officials or intelligence workers as unregistered agents as they enter the country through the fingerprint scanners at passport control and screening stations. Having this data to identify US government employees could lead to many blown covers and the aborting of several intelligence operations and missions. Another consequence of the compromised biometric information is the ability to access devices and accounts associated with such biometrics. Such devices include Apple and Samsung Galaxy cellular phones, as well as laptops. Many banks are now using fingerprint authentication methods for accessing account information via mobile devices, including J.P Morgan, and Chase & Co. Most importantly, assuming that the Chinese are behind the OPM hack, one must conclude that they now have the appropriate information to identify and contact individuals within the US federal government for purposes of monitoring their activity or even recruit them as witting or unwitting intelligence agents.

The relationship between China and the United States is fragile. Although the two powers agree on a number of strategic concerns, areas of disagreement between the two are broad and intense. In recent years the US and China have cooperated on humanitarian rescue missions, counter-terrorism, peacekeeping and nuclear nonproliferation, especially in relation to North Korea. With these common interests in mind, the two powers appear to strive to cooperate and avoid confrontation and conflict. Core issues frequently arise, however, on which Washington and Beijing do not agree. For example, the US does not support China's goal in annexing Taiwan, which Beijing believes should be under its control. Another major area of disagreement involves territorial disputes in the South China Sea and China's strategic intentions of building artificial islands in that area. Historically, ideological disputes have arisen between the People's Republic of China, nominally a communist country, and the US, which describes itself as a capitalist democracy. Throughout history, these differences have led to direct and indirect wars between the two countries, notably in Korea in the 1950s and Vietnam in the 1960s and 1970s. However, there have been attempts at rapprochement, as was the case during the Administrations of US President Richard Nixon. In essence, both countries acknowledge that a conflict between them would be disastrous, and appear to believe that their common interests lie in maintaining regional stability and continuing to develop relations with one another. [9]

According to the US Department of Defense (DoD) *Cyber Strategy* report, which was published in April 2015, the US is taking multiple steps to secure its cyber realm from hackers. Some defensive measures it is taking thus far include efforts to establish international guidelines for cyber conflict, similar to those that are in place for conventional war.[10] The goal is to eliminate the gray space that is currently lurking in the cyber world. The idea is that, by establishing and maintaining these rules or laws, cyber threats and attacks can be limited and can thus prevent the victimization of civilians. The way that the US intends to implement these guidelines is unclear. However, the US is taking other measures to secure its cyber realm, such as the use of deterrence measures. Deterrence is difficult to accomplish in cyberspace because it is not easy to determine who is attacking, or who intends to attack. Therefore, deterring a potential adversary from an attack is a complex task. According to the DoD *Cyber Strategy* document, the US must "develop effective defensive capabilities to deny a potential attack from succeeding and strengthen the overall resilience of the US systems to withstand a potential attack if it penetrates the US defenses." [11]

The report refers to one of these strategies as "deterrence by denial" which is essentially making a defensive system so efficient and effective that attackers will give up trying to penetrate the system in aggravation and frustration. Another strategy they referred to using was "resilience". That means building systems that are sturdy enough to withstand and survive cyber attacks. A problem that the US technology infrastructure faces is that its safety is mostly in the hands of the private sector since most of the government's capabilities and strategy is still classified information. This is important because private companies are in the front lines of the cyber domain and have the most to lose. They pose the most vulnerable target to hackers if certain security measures are not taken. This front line position, however, is sometimes seen as a vantage point. According to one observer, "the role of private industry is to innovate and mitigate threats, building security into applications and systems, and educating and raising awareness."[12] It is not clear

yet if these capabilities will cover private, and even military systems. Some simple ways that one can go about securing a system is limiting access to data to those who really have a need to access it and bringing in professional hackers to try and penetrate systems to detect weak spots before adversaries do. An issue that arises with the gray space that still exists is the black market for destructive malware that can detect flaws and vulnerabilities in systems and allows hackers to exploit them and gain full control. This uncontrolled market allows nation states, individuals, or non-state actors to get their hands on destructive malware. These malware programs are referred to as "zero day exploits".

Given official government rhetoric in the US, one would be excused for thinking that it would be in America's best defensive interest to try and eliminate the market for destructive malware. However, the US has allegedly used "zero day" exploits before to its own offensive benefit. The instance where the US is suspected of having used the "zero day" exploit market was in preparation for the Stuxnet virus attack that occurred in 2010. This was allegedly a joint Israeli and US operation that used several "zero day" exploits to attack the Natanz underground Iranian nuclear plant that was refining uranium. The virus was injected into the system through a USB drive, believed to have been delivered by an Israeli double agent working at the plant. The virus then spread to roughly a fifth of Iran's nuclear centrifuges. [13]

The US has expressed in the DoD *Cyber Strategy* document that it is willing to attack other countries' cyber realm if necessary. It says: "there may be times when the President or the Secretary of Defense may determine that would appropriate for the US military to conduct cyber operations to disrupt an adversary's military related networks or infrastructure so that the US military can protect US interests in an area of operations".[14] Not surprisingly, the document released by the DoD did not mention the US capabilities of offensive attacks. The US does recognize that if it carries out an attack, it ultimately gives permission to other countries to carry out attacks as well. It is no secret that the US takes an offensive approach to the cyber world, however its capabilities and methods remain undisclosed. The National Security Agency's (NSA) Tailored Access Operations (TAO) is just one of many units tasked with carrying out some of these secret tasks. [15] The TAO is government hacking unit within the National Security Agency (NSA). This program is both highly secret and important. They are tasked with hacking into foreign target's phones, and computers. They then steal information and monitor communications. They could, but it remains unknown, also be responsible for creating offensive programs that could damage or destroy foreign targets computers and networks.[16]

The complexity of offensive measures renders them unpredictable and thus often unsuccessful in the cyber domain. At the same time, deterrence, in its traditional sense, is meaningless without an absolute identification of a target. As one observer noted recently, "Deterrence is possible. But it doesn't come from force or trying to instill fear."[17] The best form of deterrence against cyber attacks is to make data and information systems so secure, that penetration is exasperating to the point of resignation. This security can only come from strong information assurance mechanisms. Additionally, taking offensive measures against an alleged perpetrator, in this case China, may jeopardize an already fragile relationship. As one expert noted, "Determining an actor (and actor's motivation) involved in a cyber incident can help guide how the United States responds."[18] But an investigation to uncover the perpetrator may only be led by law enforcement, using the devices of the criminal justice system, if the perpetrator is believed to be motivated by monetary gain. On the other hand, "If the perpetrator is deemed to be a state-sponsored actor with a different motivation, the United States may utilize diplomatic or military tools in its response."[19]

The US has to be very cautious about whom it points to as being responsible for hacks like the one directed at the OPM. China has already questioned the speculation of being involved with the breaches without explicitly denying being involved. China referred to the accusation as neither "responsible nor scientific."[20] The US lacks hard evidence thus far in the case; however, "under international law, the standard of evidence for state responsibility is solely based upon "reasonableness" versus proof beyond a reasonable doubt."[21] This could harm diplomatic relations as the Chinese are famous for their use of *Guanxi* within diplomacy. *Guanxi* is the reliance on a previously established relationship for influence within a negotiation.[22] Rejecting this friendship by insulting the Chinese may result in the "loss of face" of the Chinese. "Loss of face" is another way the Chinese describe humiliation, which is viewed as the ultimate dishonor.[23] This is one of the main reasons offensive retaliations may not be the best choice for the US. Lack of conclusive proof of the identity the attacker is the greatest complication in the OPM hack case.

Realizing that defensive countermeasures may be the best option, the US federal government has already taken multiple steps to improve cybersecurity. These four actions include establishing the National Background Investigations Bureau (NBIB), implementing a 30-day "Cybersecurity Sprint", implementing a 60-day "Clean Slate Review", and putting together a Cybersecurity Strategy Implementation Plan (CSIP). The first of these actions, the establishment of the NBIB, was intended to "concentrate solely on providing effective, efficient, and secure background investigations for the Federal Government"[24] According to the official report, the Bureau's information technology systems will be built, secured, and managed by the DoD, so as to "leverage the DoD's significant national security, IT, and cybersecurity expertise."[25] This new department is intended to also help improve how the government currently dispenses security clearances. Efforts that will continue the agenda include the following: establishing a five-

year reinvestigation requirement for all individuals with a security clearance; reducing the number of active security clearances by 17%; launching programs that constantly reevaluate personnel with clearances to decide if individuals remain eligible; and developing proposals that encourage more information-sharing between state, local, and federal law enforcement agencies when conducting background investigations. Secondly, both the 30-day Cybersecurity Sprint and the 60-day Clean Slate review are aimed at assessing the policies and strategies already in place in attempts to look for weaknesses. Lastly, the CSIP is a design that lays out both the five objectives to improve cybersecurity, and the actions that can be taken to reach those goals.

Across the IA discipline, there is disagreement on one of the major concepts within the field, namely the defense-in-depth strategy. This is a defense method that is composed of multiple countermeasures of varying complexity, application, and rigor.[26] The main argument is the absence of efficient implementation, rather than the lack of a sufficient concept. When the internet was first invented, security was not the initial principle. Rather, "it was only later that security protocols and procedures were ad-hoc bolted onto TCP/IP [...]. It was only natural for the military and government agencies to adopt what they already knew and understood."[27] This strategy, however, is now up for debate as the best defense plan. Not only are hackers able to access the same tools, strategies, and practices, but they also are able to "fly under the radar and establish persistence in a network."[28] Moreover, the human mind is the greatest weakness. "Human nature enables attackers to use social engineering and tempt people with irresistible bait that dupes the end user into being an unwilling participant in their illicit activities."[29]

So the question arises, what strategy can truly defeat all adversaries? Unfortunately, there is no "silver bullet" in information assurance. "The best IT security professionals can hope for is products and services that are highly effective, and then have overlapping technologies, or Defense in Breadth, that complement one another."[30] This strategy, however, is still not 100 percent effective. The method of "Sustained Cyber Siege" is thus introduced. This strategy promotes the use of multi-vendor approaches to People, Processes, and Technology. Essentially, the combination of defense-in-depth and defense-in-breadth would be the optimum strategy for minimum intrusions by adversaries. This new proposal, however, would require private companies to work together in order to cover each other's tracks. As the elimination of free-market competition does not seem to be a realistic option, the government is offering tax breaks and incentives as a way of promoting information-sharing between rival companies. In addition to working with other private companies, the Cyberspace Policy Review suggests information sharing with the government sector as well. "Industry and governments share the responsibility for the security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies."[31] The development of these strategies and their implementation will take time; however, the end result of a drop in intrusions would demonstrate the effectiveness IA is cable of having.

4. Conclusion

This paper used the recent OPM hack as a case study in cyber espionage and IA, because of its unprecedented importance. It not only points out the vulnerabilities in US government security systems, but the results of the hack could have potentially catastrophic consequences for American national security. The case also demonstrates the complexities and contradictions in the relationship between the US and China. Assuming that China is indeed the perpetrator of the OPM hack, the US could react in two main ways, offensively or defensively. However, this paper argues that the implementation of defensive security measures, through the expansion of IA operations, is prudent for two reasons: first because they have a higher potential of actually securing classified information; and second, because they are less likely to jeopardize America's delicate relationship with China. Even though China and the US have numerous differences, they both recognize that a conflict between them would be disastrous, and appear to believe that their common interests lie in maintaining regional stability and continuing to develop relations with one another. Therefore, taking offensive measures against an alleged perpetrator, in this case China, may jeopardize an already fragile relationship between Washington and Beijing. In fact, the US already seems to have acknowledged this reality and to have realized that defensive countermeasures may be the most fruitful option;the US federal government has already taken multiple steps to improve cybersecurity. We believe that such methods are far more effective in assuring American national security than the deployment of offensive cyber operations.

5. Acknowledgements

The author(s) wish to express their appreciation to the Department of Politics and Geography at Coastal Carolina University for their constant support and determination to help students succeed. They would also like to thank all the staff and faculty of the Intelligence and National Security program for constantly challenging and motivating them as academics, and hopeful future employees in the intelligence community. The authors would lastly like to thank Dr. Joseph Fitsanakis for his contributions in helping their academic career thrive. Not only did they take away lessons from the classroom, but also from his personal experience and expertise. This paper would not have been made possible without the guidance and critique from Dr. Fitsanakis.

6. References

1. Office of Personnel Management, "Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident," Latest News, September 23, 2015, https://www.opm.gov/news/releases/2015/09/cyber-statement-923/
2. Prescott E. Small, "Defense in Depth: An Impractical Strategy for a Cyber World," 5-6, 2011, https://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896
3. Defense Personnel Security Research Center, "Cyber Espionage," Online Guide to Security Responsibilities, http://www.dhra.mil/perserec/osg/counterintelligence/cyber-espionage.htm
4. U.S. Strategic Command Staff, "U.S. Cyber Command," U.S. Strategic Command, March 2015, https://www.stratcom.mil/factsheets/2/Cyber_Command/
5. Office of Personnel Management Staff, "Our Agency," https://www.opm.gov/about-us/
6. W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale, and Don Welsh, "A Model for Information Assurance: An Integrated Approach," June 5-6, 2001, http://grothoff.org/christian/teaching/2007/3704/w2c3.pdf
7. Corey Schou and Steven Hernandez, Information Assurance Handbook (Iowa: McGraw-Hill Education, 2015) 27.
8. Ellen Nakashima, "Chinese Government Has Arrested Hackers it Says Breached OPM Database," The Washington Post, December 2, 2015, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html
9. Bonnie S. Glaser, "Us-China Relations," Southeast Asian Affairs (2014): 76-82, http://eds.b.ebscohost.com.login.library.coastal.edu:2048/ehost/pdfviewer/pdfviewer?sid=e7a30965-c169-4042-ab69-3f60e302ee0e%40sessionmgr102&vid=7&hid=126
10. The Department of Defense, "Cyber Strategy," 34, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
11. The Department of Defense, "Cyber Strategy," 19, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
12. Jennifer Addison, "The Private Sector's Role in Cyber Security," Center for National Policy, http://cnponline.org/p/the-private-sectors-role-in-cyber-security/
13. Michael B. Kelley, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," Business Insider, November 20, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
14. The Department of Defense, "Cyber Strategy," 13, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
15. Joseph Fitsanakis, "Secretive US cyber unit has been spying on China for 15 years," Intel News, June 14, 2013, http://intelnews.org/2013/06/14/01-1278/
16. Peterson, Andrea. "The NSA Has Its Own Team of Elite Hackers." Washington Post. August 29, 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/.
17. Jeffrey Carr, "Cyber Attacks: Why Retaliating Against China Is the Wrong Reaction," The Diplomat, August 6, 2015, http://thediplomat.com/2015/08/cyber-attacks-why-retaliating-against-china-is-the-wrong-reaction/

18. Congressional Research Service, “Cyber Intrusion into U.S. Office of Personnel Management: In Brief,“ 5, July 17, 2015, http://www.fas.org/sgp/crs/natsec/R44111.pdf
19. Ibid., 5.
20. Ibid., 6.
21. Jeffrey Carr, "Cyber Attacks: Why Retaliating Against China Is the Wrong Reaction," The Diplomat, August 6, 2015, http://thediplomat.com/2015/08/cyber-attacks-why-retaliating-against-china-is-the-wrong-reaction/
22. Raymond Cohen, Negotiating Across Cultures (Washington D.C.: United States Institute of Peace Press, 1997), 71.
23. Raymond Cohen, Negotiating Across Cultures (Washington D.C.: United States Institute of Peace Press, 1997), 76.
24. Office of Personnel Management Staff, “FACT SHEET: Modernizing & Strengthening the Security & Effectiveness of Federal Background Investigations,” January 22, 2016, https://www.opm.gov/news/releases/2016/01/fact-sheet-modernizing-strengthening-the-security-effectiveness-of-federal-background-investigations/
25. Ibid.
26. Corey Schou and Steven Hernandez, Information Assurance Handbook (Iowa: McGraw-Hill Education, 2015) 25.
27. Prescott E. Small, “Defense in Depth: An Impractical Strategy for a Cyber World,” 10, 2011, https://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896
28. Ibid., 11.
29. Ibid., 12.
30. Ibid., 13.
31. The White House, “Cyberspace Policy Review,” 27, 2016, https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf