Cyber security Impacts on the U.S. National Security

Edward Gauvin

CyberIntel/CyberSecurity

April 20, 2016

Abstract

Nearly $10 billion is spent each year by the government in an attempt to keep privileged information private and free from cyber-attacks. However, a recent report indicates that at least half of the government breaches have occurred in the last four years and have been found to be caused by government employees and contractors. According to other reports, cyber-crimes have trumped terrorism as the biggest threat to a nation’s security. The efforts of protecting sensitive information are falling short as employees continue to undermine the defense efforts being put in place. People are being tricked into allowing malicious malware unintentionally and sharing private information. Despite their origins, security events are becoming more frequent causing more problems than before from federal data breaches to lose of financial data. In the current digital age, governments have critical interests of cyber security interests with many of the issues conducted by the National Security Agency, the Federal Bureau of Investigation, and the Central Intelligent Agency, among other federal firms. The paper seeks to address how cyber security has increased national insecurities impacting a nation’s economy and political systems. Additionally, cyber security has been explained from the beginning to the current adverse conditions that are posing dangers to the future years to come. Therefore, the federal government and the private sector are trying to look for ways that would reduce and prevent the negative impacts of cyber securities.

**Cyber Security Impacts on the U.S. National Security**

Introduction

The increasing dependency on information technology systems and networking pervades every significant advantage as the dependency creates vulnerabilities to cyber-based threats. As a result, underscoring the significance of safeguarding important information systems that support the nation’s critical infrastructure is a designated high-risk area[[1]](#footnote-1). The information of Information and Communication Technology industry has grown over the last years and technology is rapidly becoming a part of every facet of the modern society. Not only has the IT industry grown in capacity, but has also grown in availability, affordability, and convenience. Since the ICT devices and components are interdependent, the disruption of one component will lead to the disruption of the other components as well. As a result, there have been growing concerns about the issue of protecting the ICT systems from cyber-attacks that are said to be rapidly growing. The attacks can manifest themselves as physical damage, psychological trauma, economic losses or security breaches. Billions have been lost each year due to cyber-attacks slowing economic developments of nations[[2]](#footnote-2). The act of protecting the ICT devices is what is now known as cyber security. The broad and fuzzy concept is useful but tends to defy its precise definition. The issue of cyber security has arguably conflated with concepts such as information sharing, privacy, as well as gathering and monitoring intelligence. Nonetheless, cyber security is considered to be an important tool in protecting the privacy and unauthorized surveillance alongside sharing of information and gathering intelligence.

With this in mind, government agencies and private entities that conduct businesses through the Internet are trying to take strategic approaches to managing cyber risks. The Department of Homeland Security established a control program to set rules that govern the cyber activities in a bid to prevent and control threats from attackers. In the same way, private companies are trying to seek ways of having active defense strategies to prevent the cyber-attacks. The approaches reflect common interests in pursuing every necessary mean of preventing the disruptive activities of cyber crimes. The concepts of cyber security have joined with broad national entities to protect public and private entities[[3]](#footnote-3). Therefore, the role of the federal government involves securing both federal systems and non-federal systems. Under the current law, all federal agencies have cybersecurity responsibilities and sector-specific responsibilities as well.

**The Concept of Cyber Security**

Experts and policy makers have expressed increasing alarms about protecting ICT frameworks from cyber-attacks. This has become very disturbing so much so that the numbers of cyber-attacks are expected to increase continually in the future years[[4]](#footnote-4). Cyber security could be referred to as measures to protect against an impending attack of disruption of the IT components or any other element in the cyberspace. In other words, cyber security is the state of being protected from the threat. Therefore, cyber security aims at providing integrity by guarding against information manipulation or destruction. Also, the move is to give confidentiality through restricted access to unauthorized information that is regarded as highly essential. As a result, there is timely and reliable access to information. Cyber security is good, but the sharing of information that others may deem to be confidential and highly classified makes it susceptible to risks. This means that the risks involved in cyber security are high just in the same way that cybers security is effective.

Cyber Security Risks

People involved in cyber-attacks are either criminal with the intent of theft or extortion, spies with the aim of stealing classified information used by the government and private corporations, or nationwide state warriors who manage cyber security to support a country’s objectives. Other national threats known to be associated with cyber security include hackers and terrorists who engage in cyber-attacks in a bid to cause chaos and disruption. The IT systems are very complicated, and attackers are constantly probing for weaknesses and loopholes they would get to take advantage[[5]](#footnote-5). Defenders of the systems security are effectively working but have failed in major areas of ensuring there is no interference with major activities. As a result, it has become hard to manage intentional actions by insiders with access to systems as well as preventing supply chain vulnerabilities. Therefore, preventing malicious insertions of software or hardware during acquisition becomes a problem. The more the technology develops, the more cyber-attackers are becoming smart in using sophisticated methods of attack. A successful cyber-attack can compromise the confidentiality, integrity, and availability of an IT system regarding the information it handles. Therefore, high-risk data such as financials, proprietary information, classified governmental information, as well as personal information is prone to theft, disruption or manipulation that ultimately alters normal system operations[[6]](#footnote-6). In some instances, denial of service attacks either slow or prevent legitimate users from accessing important information. Other malware can give attackers full control over a system or completely destroy equipment being controlled. However, most cyber-attacks have limiting impacts, but any small impact successfully destroys critical infrastructure particularly in the private sector. Subsequently, the economy and livelihood of citizens are at stake. Therefore, reducing cyber-attacks involves removing the source of threat, addressing the vulnerabilities, lessening the impacts of the attacks

Cyber Weapons

The severity of disruption may range from low to high depending on the tools that have been employed in the Cyber-attacks. In the same way, the actors who employ these tools could be individuals, groups or even nations. Perhaps the most common cyber weapon is malware used to refer to any malicious software. For instance, Bots, viruses, and worms are examples of malware. On the other hand, botnets are programs that link computers together and affect the entire chain once one is attacked. Also, the distributed denial of service attacks floods their targets with a request which when accepted results to service outages. Finally, the automated defense systems that are network responses widely used in the private sector are presented as DODs having offensive operations that interfere with computer systems[[7]](#footnote-7).

Targets

The challenge of cybersecurity is that it has been failing to uphold and effectively implement the required standards in maintaining national security. As a result, there have been increasing alarms about how cyber security approaches could be effectively implemented to reduce control the impact of cyber security. Within the context of cyber warfare, two major areas have been the focus of cyber-attacks that in turn causes significant impacts to a country’s information systems. Government and military networks have been for a very long time targeted to steal data to gain an intelligent advantage or plan a malicious threat that could cause a disruption in the military operations. At one time, the Pentagon had a massive breach that required an entire clean up to remove the threat and prevent others from attacking their systems. While the threat was associated with espionage and loss of sensitive information, there might have been possibilities of malware been planted to disable communications[[8]](#footnote-8). The other most targeted sector is the critical infrastructure and industrial control systems. The critical civilian infrastructure encompasses networks and services considered to be a critical component of the nation but owned and managed by the private industry. Sectors such as energy, transportation, food supplies, and communications are very vulnerable to cyber-attacks since the attackers know the economy could be crippled. They are also very vulnerable since they rely on open-source software with interconnected networks. In the same way, the large-scale industrial control systems such as data acquisition systems are very much prone to cyber-attacks. This is so because the systems provide real-time information to remote operators. The capabilities of the remotely-controlled industry make the machines vulnerable to attacks. The cyber-attacks that target the IT are different from those that target the OT since OT systems produce kinetic effects. Also, the OT environments involve very high networking environments adding up to the complications of training personnel and marinating the systems[[9]](#footnote-9).

**Potential Impacts**

The U.S. government is expected to spend an estimated of $65 billion on cyber security contracts in the next six years[[10]](#footnote-10). Experts believe this would be so due to the numerous hacking who launch attacks for many different reasons. Any malicious attacks from petty thieves could launch a significant attack against the U.S. As a result, the FBI has raised flashed warnings to business owners advocating them to launch a campaign against malware attacks. Still, it is unclear as to who is behind the attacks. As the years progress, the attacks have grown to be more sophisticated. Organizations are at a point where they are expected any type of finely-tuned attack on a regular basis. Most people feel that continuous threats from cyber-attacks are rapidly increasing with the ability to impact economic stability and national security as well. The attackers are constantly forming new ways of creating cyber-attacks prompting companies to be on high alert by employing strict measures on their internal control systems[[11]](#footnote-11).

Due to this, the U.S. government is calling for more collaborative actions with the private sector to reduce and mitigate the effects of the cyberthreats to the nation’s critical infrastructure. In this regard, measures of establishing standards are being put in place to bring developments in the cybersecurity frameworks. However, potential liabilities arise with breach notifications and security laws that result from government sharing programs. Also, there are uncertainties with about the kinds of standards that will be set to establish protection of critical infrastructure. The standards may not be in line with the framework with the possibilities of a dilemma regarding full participation in the set programs. Companies will have to decide whether to adhere to the information sharing initiatives or set their violation privacy laws. All these measures are bound to increase federal costs in the future.

**A History of Cyber Security**

Unfortunately, nearly everyone who is using a computer is familiar with malware, viruses and other disruptive forms of hacking. Cyber-attacks have become a commonplace in the lives of people and businesses altogether. In the past, most computer users did not think much about protecting their personal information from online theft, but cyber-attacks have already made their way through t our systems. Syndicates have been launching attacks against companies for decades that have resulted in the loss of billions each year[[12]](#footnote-12). Even though the threats have been present for a long time, the intensity is increasing as organized crimes as attackers target everything from credit card data to entire infrastructure. From presidents Regan to Bush, national figures have in the front line to prevent cyber-attacks that impact the overall national security. Following the Oklahoma bombings, President Clinton set up the President’s Commission on Critical Infrastructure Protection in the mid-1990s to safeguard vital systems such as natural resources, transportation, telecommunication, among other sectors to prevent an economic downfall[[13]](#footnote-13). It is evident that lack of security in a nation leads to poor performance of national sectors.

Policy reforms have been changing since then with every manifestation of attacks, but the crippling impact is still taking a toll in nations. From past years, bills have been drafted and passed in an attempt to prevent cyber-attacks on our computer systems. This was so much needed especially due to the Morris worm that was launched in 1989 and affected close to 600,000 computers[[14]](#footnote-14). The efforts have been increasingly implemented as seen with the FBI raid on more than a dozen homes in 1983[[15]](#footnote-15). There is no stop to the continuously increasing efforts as new forms of threats are manifested each day. In the past, national security was considered to be the responsibility of the government. The new age of security has changed that thinking as national security has now become the responsibility of everyone including private entities. Both the private entities and the government are stepping up their strategies with calculated precision as more people are progressively becoming more aware of the dangers that come with using the Internet and telecommunication devices. Staffs are being trained to uphold information security especially since simple devices such as mobile phones pose great threats to an organization’s internal control systems[[16]](#footnote-16).

**Political Agendas Served by Cyber Security**

Why does it seem that cyber security is becoming an important part of national politics, geopolitics, and international relations? Any threat to national security is a threat to the political stability of any nation. Data is fuel for digital transformations as nations are coupled with shared responsibilities since cyber threats do not respect borders. Over time, cyber security has been continued to be on political agendas and influence how the changing governments form and implement new political strategies to address the problem. This is probably so because the disruptions of cyber security interfere with the development of a nation. Cyber incidences are real and cause problems for the business communities causing major inconveniences. Additionally, cyber threats have interfered with international relations between countries. If the frictions between nations are not taken care of, economies will fall, and trade will be reduced. Cybersecurity problems have been seen to affect the U.S. and China relations, particularly as seen with the Brookings project[[17]](#footnote-17). National borders are already porous as the real world seems non-existent in cyberspace. For the United States, security forces had to oppose the new threat giving it low priority making old security political strategies obsolete. As stated above, the Oklahoma bombings led to the creation of the PCCIP with the issue of cyber security remaining top in political agendas. The Bush administration followed with the political strategy of physical threats of terrorism but progressively accommodated Clinton’s Presidential Commission on Critical Infrastructure Protection. National security, particularly on cyber threats, became the responsibility of the government, the military, as well as the intelligent committee[[18]](#footnote-18).

When there are tensions, countries tend to rely on asymmetrical vectors that would provide such nations with benefits. There will be people in the region that will either be sponsored by the government to exploit the country’s capabilities. A good example could be that of someone hacking into the military through the Internet to steal military and technological information. The entry barrier is very low, but the potential impact on national security is high. Moreover, it is very hard for the hacker to be caught. Therefore, CIOs and CTOs should pay most attention if they are looking to upgrade their security measures[[19]](#footnote-19).

**Issues Generated by Cyber Security**

Cyber security issues continue to grow and manifest in various ways. The most notable event was the formation of the Zeus virus that saw financial fraud of hundreds of people and financial institutions. Nearly 1.2 million computers were affected stealing account numbers, passwords, personal identification numbers, and other confidential information to steal finances from people. In almost the same way, the most expensive virus is said to restrict control to devices once infected. Nearly 99% of all computer systems are prone to cyber-attacks, and 68% of funds lost due to cyber-attacks have never been recovered[[20]](#footnote-20). Another most notable problem are insider threats where employees who have access to organizational systems cause distortion, theft, and loss of critical information creating huge losses for companies. The inside attacks are either intentional or ignorance by workers to maintain information security. What is also more alarming is the fact that the government is making people more vulnerable. The sharing of information that most people consider to be private provides a loophole for people to either steal or distort the information. People are not secure with private firms having private information as there is a continuous battle between governmental agencies and private firms. Private firms are only required to give out private information if authorized by the owner or for national security reasons. Apart from these two factors, private firms are required to safeguard the personal information of their clients with the highest possible security.

Long-Term Challenges

As stated above, cyber security activities involve preventing cyber disasters, reducing the impacts of successful attacks, improving international collaboration, clarifying clear roles of agencies as well as fighting cyber-crimes. Experts say that effective security is a major part of the ICT design; yet, developers have focused on other features than design for their economic reasons. Also, many future security requirements cannot be easily predicted posing a different challenge for designers to develop[[21]](#footnote-21). The structure of the economic incentive is also has been for a long time been distorted. Cyber-crime is considered as cheap, profitable, and comparatively safe for cyber criminals to carry out. Conversely, cyber security can be expensive and imperfect while the economic returns of controlling the problem are unsure. Implementation of cyber security measures is not easy since it is difficult for shareholders to come to a consensus with their different understanding and approaches to cyber security. Finally, the growing technology still poses numerous threats to the effective implementation of cyber security measures[[22]](#footnote-22). New emerging technologies such as big data, cloud computing, mobile computing, social media, and the Internet of things further complicate the current problem. Technological advancements do not only bring improved performance but also brings more threats since cyber-attacks will take more complicated and sophisticated forms. This, therefore, means that growing technologies will also bring more cyber-attacks. Maintaining cyber security measures is continually becoming a problem. For instance, the growing big data has led to cloud computing creating more easy avenues for cyber-attacks to be carried out[[23]](#footnote-23).

Table 1: FISMA and IT spending

Billions of dollars, (FY)2006 to 2013

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Fiscal year  | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
| FISMA spending  | 5.5 | 5.9 | 6.2 | 6.8 | 12.0 | 13.3 | 14.6 | 10.3 |
| Total IT spending  | 66.2 | 68.2 | 72.8 | 76.1 | 80.7 | 76.0 | 75.0 | 73.2 |
| FISMA proportion of total IT spending (%) | 8.3 | 8.7 | 8.5 | 8.9 | 14.9 | 17.5 | 19.5 | 13.8 |

Source:

Data on FISMA spending from the Office of Management and Budget (OMB), (Found in the Office of Management and Budget,

**Documents Defining the U.S. government Strategy in Cyberspace**

According to the United States government, cyberspace is known to be known to be a global domain with networks is interdependent and encompasses all IT components[[24]](#footnote-24). Attacks launched against the cyberspace have been on the rise with a wide variety of participating actors using a variety of methods. In the same rate, the United States has been increasingly reliant on the Information Technology as well critical networked infrastructural components. Therefore, is the country effectively organized to defend its needs? Cyberspace entails important components of infrastructure, commerce, the government as well as national security. Also, since cyberspace goes beyond geographical boundaries, it becomes difficult for the United States government to control the influence of cyberspace.

Therefore, the Department of Homeland Security is the governing body responsible for securing a nation’s digital assets. But, the Department of Defense plays a big role in the cyberspace defense. The National Military Strategy for Cyberspace Operations gives the DOD orders to defend the Department of Homeland Security as well as supporting other key infrastructural resources. DOD oversees its defense strategies its information networks and other specific defense agencies. The multiple strategy documents and directives give directive guidelines to the conduct of military operations in cyberspace. However, the cyberspace defense is still evolving. The documents seek to illuminate various aspects of the United States military operations in cyberspace. They are considered to be an important part of expanding education on issues regarding cyber security. They address the language of cyberspace, visions, and strategies, activities and responsibilities, computer network defense systems, intelligence operations, as well as the military cyber organization[[25]](#footnote-25).

With this in mind, document one gives nearly 50 definitions of the cyberspace operations that also include weapons. The joint Chief of Staff also issued document ten that contains joint terminologies of all cyberspace operations. The two documents provide readers with extensive accounts of definitions associated with cyberspace operations in a bid to establish common terms for the discipline. On the other hand, visions and strategy documents include documents 17, 27, 25, 4,7,16 and 26. The DOD cyber strategy found in document 25 gives five strategic goals and capabilities of cyberspace operations. It also gives steps of how the operations should be carried out as well offering an assessment of the cyber strategies and its capabilities. The U.S. Cyber Command’s vision statement found in document 27 focuses on the strengthening of partnerships with other defense agencies to support joint force operations[[26]](#footnote-26). Also, document 4 of the United States Airforce Blueprint for Cyberspace Operations gives joint and presidential guidelines on the Air Force concepts of cyberspace. The most recent document is documented 26 that specify governmental priorities of defending cyberspace operations, protecting infrastructure and enabling operations. Additionally, document 6 launched by STRATCOM in 2009 gives the responsibilities and command relationships with a document giving the full operational capabilities and key missions with some being classified. In relation, document 9 declares the general orders of the Army Cyber Command while document 11 shows the assigning control of information operations command. Document 5 provides a brief information and graphics of the entire operations while document 13 gives a memorandum of the divisions’ greater focus on cyber issues such as intelligence, surveillance, and reconnaissance that provides support to defending cyberspace operations. Activities and responsibilities of the U.S. Cyber Command in document 12 provide relevance and concepts of the tasks. In the same regard, document 15 of the Air Force Directive discusses the responsibilities of the Air Staff components, Command, legal units, as well as other organizations. A restricted publication of document 18 was issued immediately on the restricted information of the operations related to cyberspace, the national intelligence, authorities and other relevant information regarding the U.S. government and multinational organizations[[27]](#footnote-27). Similarly, document 23 states all instructions issued to relevant cyberspace agencies. It additionally gives a list of all 132 U.S. government documents relevant to the DOD cyber security organizations and their activities.

As illustrated by document 20, responsibilities within each organization is delineated to report and respond to incidences effectively. Consequently, document two was issued to report on how incidents should be handled with a diagrammatic representation of its seven different enclosures of how the methods are handled. Forensic and network analysis, as well as the examination of legal issues, are also part of the document. Finally, documents 19 and 3 are involved in the intelligence and counterintelligence. Secret instructions on cyberspace operations are in document 19 alongside the responsibilities of the various components of the DOD while document 3 is known as the strategy document due to its mission objectives of the cyberspace operations. These documents clearly show the capabilities of the U.S. government addressing the issues of cyberspace[[28]](#footnote-28). The government has full resources at its disposal that include both technological equipment, and human resources. Therefore, the government can handle the cyber security problems but will still require tighter measures to govern federal employees concerning access to classified and other important information.

**Organizations Responsible For Maintaining Cyber Security**

As stated above, the main federal agency responsible for overseeing cybersecurity measures is the Department of Homeland Security also known as the DHS. Subsidiary organizations of the Federal Bureau of Investigations and the Central Intelligence unit help in Department Of Defense to effectively implement the stated cyber security measures. The Department of Defense responds to the Department of Homeland Security after liaising with the FBI and the CIA. However, the Federal Bureau of Investigations deals with national security measures such as the cyber security problems while the Central Intelligence Agency is concerned with a gathering of information at an international level that relates to the security. Despite the different organized tasks of the departments, they work together when need be to oversee both national and international problems do not compromise the national security of the U.S. Additionally, executive authorities involve both the president-elect and the White House Chief of Staff is also involved in ensuring national security is upheld in the best possible manner. They are also responsible for drafting security bills and issuing documents that define cyberspace strategic operations and rules. Finally, the U.S. military is concerned with the implementation of the cyberspace operations as stated in the 27 documents that define cyberspace operations and policies. However, they receive directions from the United States Secretary of Defense such as carrying out clandestine operations in cyberspace. According to the DOD, a clandestine operation is a fully sponsored governmental operation that is conducted in utmost secrecy. Apart from the U.S. governmental agencies, international agencies are also involved even though there is no clear directive to the extent of their operations.

**Practical Aspects**

The Cyber Administrative National Security State

National security encompasses a broad range of activities ranging from military actions, diplomatic crisis, executive activities as well as secret intelligence activities aimed at preserving the sovereign interests. In the government activities, the clear definition of national security is important to prevent any misunderstandings that may arise with debatable legal issues and policy definitions. Cyber national security concerns can exist as significant problems such as stealing classified government information and selling it to terrorists undermining security stability of the U.S. As a result, such activities attract the enforcement of investigations by both the state and federal agencies under the criminal and civil laws[[29]](#footnote-29). Private companies, state and federal governments work together to ensure they properly identify and disrupt ongoing cyber threat activities that are prone to cause national security problems. Therefore, the cyber administrative national security is concerned collectively with managing diverse threats from individuals, groups, and even nations.

**Recommendations**

Legislative Bids

Since the one-eleventh Congress, different bills have been drafted with others being reformed in a bid to address cyber security issues. The bills being passed include the Information Sharing where access to classified threat information is made easy to the private sector, and barriers are removed to improve on information sharing between the federal government and the private sector. However, the roles of the Department of Homeland Security and the IC have significant impacts on the privacy issues as well as civil liberties. Also, information sharing increases the risks associated with misuse of federal information or information from the private sector. Additionally, the FISMA reform that updates the 2002 law reflects on the changes in ICT and the threat landscape. Still, the role of the Department of Homeland Security, the OMB, and Commerce explain that the reform does not meet the flexibility requirements[[30]](#footnote-30). As a result, the legislative proposed the establishment of Research and Development agencies to update agencies with authorizations and conformity to the planning requirements. However, this would mean an increase in government expenditure due to additional levels of funding. Perhaps the most suitable proposal as indicated in the legislature is an improvement in the workforce. It is important for organizations to improve the skills, size, and preparation of the federal and private sector to enhance the effectiveness of the cyber security workforce. Despite its proposed effectiveness, the hiring and retention of employees are hard and limits the roles of the Department of Homeland Security, NIST, the National Science Foundation as well as the National Security Agency. Also, privately held CI improves the protection of the private sector from attacks that have a high likelihood of causing significant impacts to the security of a nation. However, this conflicts with both the regulatory and voluntary approaches the government employs to address cyber security[[31]](#footnote-31). Data-breaching notification is also important should be employed once the systems detect breach of information particularly personal information of individuals. This may not be an easy process to implement as the state laws may conflict with federal laws regarding what responses should be used. Despite all this, the most important step is for governments to form cyber-crimes laws that are updated by the criminal laws and the law-enforcement agencies.

Other Recommendations

The federal government of the United States has taken various steps that are intended to reduce the issues that are associated to cyber security. Among the recommendations that are made to the federal government so as to reduce the case of cyber security are related to the aspects of information system control. This is because this is the weak points that are targeted by the cyber security attackers. There exist major deficiencies in the information security controls. A recommendation for this would be the establishment of access control on the information system. This will ensure that only authorized individuals will be capable of accessing the information. As such this will reduce the cases of access, manipulation of data by the unauthorized individuals[[32]](#footnote-32).

The other significant recommendation is the implementation of configuration management controls. This will ensure that only legitimate and authorized software programs. This is a critical step in preventing the vulnerability of information and, therefore, reduces the cases of cyber-based threats. In the same accord, there should be widespread implementation of agency-wide information security programs. In so doing, this will act as a framework for ensuring that the possible cyber security risks are properly understood. This will, in turn, ensure that effective controls are sought and implemented[[33]](#footnote-33).

Finally, there is the need to conduct comprehensive planning of operations. Planning will go a long way in avoiding the major disruptions. Planning, therefore, translates to enhanced security in terms of the computer-dependent operations. More so planning in conjunction with segregation of duties is recommended in this case. It is important as it will significantly reduce the risk one individual conducting inappropriate actions independently successfully for a considerable duration without detection[[34]](#footnote-34).

**Conclusion**

Cyber security has emerged to be the next problematic paradigm that requires immediate attention. The government is spending a lot to safeguard the nation’s security threats against cyber-attacks. Additionally, companies in the public and private sectors, as well as federal agencies, are losing credible amounts of information that subsequently transcends to huge financial losses. As a result, the economic performance drops affecting the politics of a country. Government officials have come up with policies that govern the way information is shared and are implemented by key government agencies such as the OMB, the Federal Bureau of Investigations, and the Central Intelligent Agency among other agencies[[35]](#footnote-35). However, the government has assigned the entire responsibilities to the Department of Homeland Security that is helped by the mentioned agencies. Cyber-attacks have been a looming problem that has surpassed terrorism activities. More so, companies are continuously relying on IT and networking activities as it is required in the current information age. The source of cyber-attacks is not clearly known as it is believed that the Internet helps in the implementation of the attacks. The problem is yet to be settled as experts and policy makers believe that the problem will escalate in the future. The growing attacks target mostly military and critical infrastructure in a bid to paralyze the economy and political systems of a country. Despite the numerous government policies and implementations, cyber security seems to fall short in its effectiveness to reduce and prevent the impacts of cyber-attacks. Still, it is important for the cyber security measures to be implemented. The growing technologies are not only developing infrastructures but also offering attackers more sophisticated ways of improving their heinous acts. As a result, the federal government should collaboratively work alongside the private sector to continuously develop new ways of counteracting the effects brought about by cyber-attacks. No threat is too small, and no protection is too strong. Therefore, every cyber security threat should be treated with caution. Everyone is prone to cyber-attacks regardless of the size or risk associated with the attack. As a result, people, firms, and the federal government should not ignore any precautions given when trying to develop a protection system with the tools and information available online. Rather, everyone should be made aware through educative materials and demonstrations that show people how to safeguard their information. Employees are also supposed to be scrutinized to ensure they do not steal, destroy, or manipulate important data for their selfish gains.

Bibliography

Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." In *Proceedings of the VDE Kongress*, vol. 116, pp. 213-218. 2004.

Chandler, Jennifer A. "Security in cyberspace: combatting distributed denial of service attacks." *University of Ottawa Law & Technology Journal* 1, no. 231 (2003): 2004.

Clements, Sam, and Harold Kirkham. "Cyber-security considerations for the smart grid." In *Power and Energy Society General Meeting, 2010 IEEE*, pp. 1-5. IEEE, 2010.

Goldsmith, Stephen, and William D. Eggers. *Governing by network: The new shape of the public sector*. Brookings Institution Press, 2005.

Jamwal, Sunny, and John McHugh. "Worm Analysis and Changes in Host Behaviors During Worm Outbreaks." In *Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS'09. World Congress on*, pp. 47-57. IEEE, 2009.

Lieberthal, Kenneth, and Wang Jisi. "Addressing US-China Strategic Distrust." (2012).

Marston, Sean, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, and Anand Ghalsasi. "Cloud computing—The business perspective." *Decision support systems* 51, no. 1 (2011): 176-189.

Mosco, Vincent. *To the cloud: Big data in a turbulent world*. Routledge, 2015.

Moteff, John, and Paul Parfomak. "Critical infrastructure and key assets: definition and identification." LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2004.

Nakashima, Ellen. "Cyber-intruder sparks massive federal response—and debate over dealing with threats." *Washington Post* 8 (2011).

Nicholson, Andrew, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. "SCADA security in the light of Cyber-Warfare." *Computers & Security* 31, no. 4 (2012): 418-436.

Obama, Barack. *National Security Strategy of the United States (2010)*. DIANE Publishing, 2010.

Paoletta, Patricia. "The Cybersecurity Overreach: A Few Harsh Words About the President’s Cybersecurity Executive Order, Along with a Better Solution."

Pursiainen, Christer. "The challenges for European critical infrastructure protection." *European Integration* 31, no. 6 (2009): 721-739.

Richelson, Jeffrey T. *The US intelligence community*. Westview Press, 2015.

Rid, Thomas, and Peter McBurney. "Cyber-weapons." *the RUSI Journal* 157, no. 1 (2012): 6-13.

Rosenzweig, Paul. "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence." *DETERRING CYBER ATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR US POLICY, National Research Council, Forthcoming* (2010).

Yang, Debra Wong, and Brian M. Hoffstadt. "Countering the cyber-crime threat." *Am. Crim. L. Rev.* 43 (2006): 201.

1. Rosenzweig, Paul. "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence." *DETERRING CYBER ATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR US POLICY, National Research Council, Forthcoming* (2010). [↑](#footnote-ref-1)
2. Goldsmith, Stephen, and William D. Eggers. *Governing by network: The new shape of the public sector*. Brookings Institution Press, 2005. [↑](#footnote-ref-2)
3. Clements, Sam, and Harold Kirkham. "Cyber-security considerations for the smart grid." In *Power and Energy Society General Meeting, 2010 IEEE*, pp. 1-5. IEEE, 2010. [↑](#footnote-ref-3)
4. Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." In *Proceedings of the VDE Kongress*, vol. 116, pp. 213-218. 2004. [↑](#footnote-ref-4)
5. Byres, Eric, and Justin Lowe, (2004) [↑](#footnote-ref-5)
6. *ibid* [↑](#footnote-ref-6)
7. Rid, Thomas, and Peter McBurney. "Cyber-weapons." *the RUSI Journal* 157, no. 1 (2012): 6-13. [↑](#footnote-ref-7)
8. Nakashima, Ellen. "Cyber-intruder sparks massive federal response—and debate over dealing with threats." *Washington Post* 8 (2011). [↑](#footnote-ref-8)
9. Nicholson, Andrew, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. "SCADA security in the light of Cyber-Warfare." *Computers & Security* 31, no. 4 (2012): 418-436. [↑](#footnote-ref-9)
10. Marston, Sean, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, and Anand Ghalsasi. "Cloud computing—The business perspective." *Decision support systems* 51, no. 1 (2011): 176-189. [↑](#footnote-ref-10)
11. Nakashima, (2011) [↑](#footnote-ref-11)
12. Marston et al., (2011) [↑](#footnote-ref-12)
13. Pursiainen, Christer. "The challenges for European critical infrastructure protection." *European Integration* 31, no. 6 (2009): 721-739. [↑](#footnote-ref-13)
14. Jamwal, Sunny, and John McHugh. "Worm Analysis and Changes in Host Behaviors During Worm Outbreaks." In *Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS'09. World Congress on*, pp. 47-57. IEEE, 2009. [↑](#footnote-ref-14)
15. Yang, Debra Wong, and Brian M. Hoffstadt. "Countering the cyber-crime threat." *Am. Crim. L. Rev.* 43 (2006): 201. [↑](#footnote-ref-15)
16. Yang, Debra, and Brian M. Hoffstadt, (2006) [↑](#footnote-ref-16)
17. Lieberthal, Kenneth, and Wang Jisi. "Addressing US-China Strategic Distrust." (2012). [↑](#footnote-ref-17)
18. Moteff, John, and Paul Parfomak. "Critical infrastructure and key assets: definition and identification." LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2004. [↑](#footnote-ref-18)
19. Yang, Debra, and Brian M. Hoffstadt, (2006) [↑](#footnote-ref-19)
20. *ibid* [↑](#footnote-ref-20)
21. Chandler, Jennifer A. "Security in cyberspace: combatting distributed denial of service attacks." *University of Ottawa Law & Technology Journal* 1, no. 231 (2003): 2004. [↑](#footnote-ref-21)
22. Rosenzweig, (2010) [↑](#footnote-ref-22)
23. Mosco, Vincent. *To the cloud: Big data in a turbulent world*. Routledge, 2015. [↑](#footnote-ref-23)
24. Chandler, (2004) [↑](#footnote-ref-24)
25. Richelson, Jeffrey T. *National Security Agency Tasked with Targeting Adversaries' Computers for Attack Since Early 1997, According to Declassified Document*. 2013. [↑](#footnote-ref-25)
26. Richelson, (2013) [↑](#footnote-ref-26)
27. *ibid* [↑](#footnote-ref-27)
28. Richelson, Jeffrey T. *The US intelligence community*. Westview Press, 2015 [↑](#footnote-ref-28)
29. Obama, Barack. *National Security Strategy of the United States (2010)*. DIANE Publishing, 2010. [↑](#footnote-ref-29)
30. Paoletta, Patricia. "The Cybersecurity Overreach: A Few Harsh Words About the President’s Cybersecurity Executive Order, Along with a Better Solution." [↑](#footnote-ref-30)
31. Paoletta, [↑](#footnote-ref-31)
32. Goldsmith, Stephen, and William D. Eggers. (2005) [↑](#footnote-ref-32)
33. Goldsmith, Stephen, and William D. Eggers. (2005) [↑](#footnote-ref-33)
34. *ibid* [↑](#footnote-ref-34)
35. Richelson, (2015) [↑](#footnote-ref-35)