Exploring the Extent to Which Cyber Security is Essential to Homeland Security

Emmanuel N. Amadi, Ph.D.
Chair, Department of Criminal Justice
Mississippi Valley State University
United States

Abstract

This article takes a close look at cyber Security for the purpose of providing information that enhances knowledge and understanding of cyber Security and explores the extent to which it is essential to homeland security. The article is for the most part a nontechnical discussion of cyber Security with a focus on the national level and with the aim of exploring the extent to which cyber Security is essential to homeland security. The motive for this exploration is the pressing issue of the potential adverse consequences of cyber attacks on the homeland. Accordingly, this article involves qualitative research that combines exploratory and descriptive research in which both cyber Security and homeland security are defined and discussed in detail. This article finds that cyber Security is to a great extent essential to homeland security because the consequences of successful cyber attacks on the homeland could be devastating to the nation's cyber infrastructure, critical infrastructure, and the American people. Cyber attacks are very serious and are increasingly threatening to homeland security as they have the potential to result in enormous social and economic damage and disruption that could jeopardize the welfare of the nation. Therefore, all stakeholders must make concerted efforts and utilize all available resources to ensure cyber Security in the effort to protect the homeland. Otherwise, the security of the nation against cyber attacks would be severely hampered.

Keywords: Petroleum.Fuels. Distribution. Logistics. Transportation.

Introduction

Cyber Security is a growing and pressing issue of homeland security. And it is an issue of great concern to leaders in government and in business and the non-profit sector. It is also a matter of great concern to security analysts, experts, and researchers. It involves efforts and measures taken to protect the homeland from cyber threats. Thus, research efforts to gain knowledge and understanding of cyber Security and to explore the extent to which it is essential to homeland security should be highly encouraged because of the potential divesting effects to homeland security by successful cyber attacks whether in the form of cybercrime, cyber terrorism, or cyber warfare. Accordingly, cyber Security here refers to security against cybercrime, cyber terrorism, and cyber warfare – all of which are dangerous to homeland security.

Our modern society relies to a large extent on computers and computer network systems in the way it operates because computers have become fixtures of our everyday life in the social, political, and economic arenas. Consequently, the term "cyber" is now used to mean anything real or virtual associated with a computer or a computer network (Taylor, Fritsch, and Liederbach, 2015). The growth and advancement of computer technology and the Internet has been fast and enormous. And our reliance on computers and the Internet will continue to increase as our "information society" continues to grow (Year, 2013; Taylor et al., 2015; Loukas, 2015; Bullock, Haddow, and Coppola, 2016). Indeed, the growth and advancement of computer technology have been a mixed blessing with enormous adverse social and economic consequences associated with it, because as noted by Taylor et al. (2015), "The same technology that provides useful services has also been perverted for criminal and terrorist purposes" (p. 2). This is so because the dynamics and processes involved in the execution of cybercrime, cyber warfare, and cyber terrorism are virtually the same as those in which computers and computer networks are used for services that are beneficial to the society. Cybercrime, cyber warfare, and cyber terrorism are increasing at an alarming rate, and that poses great danger to homeland security because any country, including the United States that has access to the Internet can fall victim to some form of these cyber threats (Taylor et al., 2015; Loukas, 2015; Bullock et al., 2016).

At this point, I provide important definitions of the two important concepts in this article: cyber Security and homeland security.

Definitions of Cyber Security and Homeland Security

There are many definitions of cyber Security provided by various experts on the subject. However, Bullock et al (2016) provide an important definition of cyber Security when they defined it as follows: "It is the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. It includes protection and restoration, when needed, of information networks and wire line, wireless, satellite, public safety answering points, and 911 communications systems and control systems" (p. 375).

On the other hand, the White House's National Strategy for Homeland Security has also provided an important definition of homeland security when it defined it as follows: "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." (cited in Dwyer, 2015, p. 1). As Dwyer has stated, "homeland security in the United States has become a centralizing aspect of government response to threat, external and internal, coordinated at a national level through the Department of Homeland Security" (2015, p. 1). According to Dwyer, prior to the terrorist attacks on September 11, 2001, homeland security was a term many Americans were unfamiliar with. However, after the 9/11 attacks, homeland security became a very familiar term among the American people, young and old alike. It has also become a field of study "wherein many college students are seeking careers in government service" (Dwyer, 2015, p. 1).

The United States Department of Homeland Security is a cabinet department of the United States federal government, created in response to the September 11 attacks, with the primary responsibilities of protecting the territory of the United States and protectorates from and responding to terrorist attacks, man-made accidents, and natural disasters (http://www.bing.com/search?q+department+of+homeland+security&form=PRUSEN&m.) Specifically, the functions of the Department of Homeland Security include coordinating the federal executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States (Martin, 2015, p. 13). In the following section, I discuss the reason why cyber Security has emerged as a grave concern.

The Emergence of Cyber Security as a Grave Concern

Cyber Security is a grave concern that emerged due to advancements in information and computer technology resulting in the interconnectedness of all people and all things, thereby increasing our reliance on computers and the Internet. As noted by Bullock et al. (2016), "Communications, commerce, finance, and all forms of information management and access can be achieved from almost anywhere, using devices so compact they fit in our pockets" (p. 321). Conversely, according to Taylor et al. (2015), "Technological progress in the areas of computing, networking, communications, and e-commerce provides criminals and terrorists with an unbelievable array of new tools and opportunities to perpetrate their crimes" (p. 2). According to the authors, the Internet seems to be a lawless space where bullies, deviants, criminals, and terrorist operate freely with little or no fear of any consequences for their actions (Taylor et al., 2015, p. 2). As our reliance on computers and the Internet continues to grow so will our vulnerability to cybercrime, cyber warfare, and cyber terrorism continue to grow because in the process of entry, storage, and retrieval of data and information on an interconnected network of computers, there exists the opportunity to steal, circumvent, manipulate, or sabotage data and information at any of these junctures (Bullock et al., 2016, p. 321).

Computers are cyber systems; and, as a consequence, securing them from cyber attacks has become a matter of homeland security because of the enormous damage that can result from failure to secure our computer and information network systems. Computer hackers have the capability to deface public sector and private sector organizations' websites, steal personal data to support multibillion dollar credit theft industry, alter traffic signal patterns, speed up and slow down trains, and so on (Bullock et al., 2016, p. 322). Cyber attacks by a nation, group, or individual can result in enormous social and/or economic damage and disruption, including physical destruction, injuries, and death. And threats from cybercriminals can pose very real risks to the economic security and privacy of the United States and its citizens (Bullock et al., 2016).

Planning cyber attacks against cyber systems does not necessarily require much planning as cyber systems can be easily accessed through the Internet. In fact, cyber systems are designed to automate processes. As a consequence, a security incident that directly affects one system can adversely affect other systems' processes (Loukas, 2015, p. 53). Cyber attacks on computer systems are made possible by the interconnectedness of computer systems and the vulnerability of their computation and communication elements. For example, a hacker can take control of the computing or communication components of water pumps, medical implants, cars, and gas pipeline valves and use that opportunity to control these systems to cause enormous damage to property or the environment and, in effect, put lives at risk (Loukas, 2015, p. 11). The section that follows discusses the process of carrying out a meaningful cyber attack successfully.

The Process of Carrying Out a Meaningful Cyber Attack Successfully

The process of successfully carrying out an effective cyber attack may require research, reconnaissance, and the ability to discover and exploit the vulnerabilities as well as the right entry points of the targeted computer system, while evading and concealing the attacker's traces. Similarities exist in cyber security threats against computer systems regardless of the source of the threat. In all cyber security threats, the attacker attempts to identify entry points from where it is possible to directly communicate with the system's actuators and sensors or indirectly impact the operation of the computer system under attack by manipulating the control and communication infrastructure of the computer system.

This, for all intents and purposes, may require considerable planning and research. Therefore, when an attacker selects a target, he/she attempts to gather useful information about the target. The information may include the Internet Provider (IP) address, the type of network infrastructure of the target, the target's types and versions of software and hardware, and so forth. The search for information usually begins with an Internet search for any information on the target that is publicly available. Often, much information about a target can be obtained online through a mere Google search. The Internet can also be a means for finding and purchasing the same type of system that the attacker is targeting. After purchasing the device, the next step is to attempt to learn the device and identify ways to breach the security of the device. Learning the purchased device facilitates planning attack against the device with a high probability of success (Loukas, 2015, pp. 146-147).

Moreover, a cyber attack can be successfully carried out by a determined attacker on a highly technically secured system, such as an industrial control system by bypassing the system's technical security protections through merely deceiving the legitimate user of the system to give out his or her password or clicking a link to a malicious web site. All the resources spent on providing strong technical protection of a system, such as firewalls, encryption and secure access devices would be wasted if the human operator of the system can be manipulated by a determined attacker into divulging critical information (Loukas, 2015, pp. 147-148). In the next section, I briefly discuss the three dimensions of cyber Security outlined here: cybercrime, cyber warfare, and cyber terrorism and their implications to homeland security.

Cybercrime

Cybercrime is a serious and increasing threat to homeland security because of the enormous social and economic consequences associated with it. It involves criminal activity in which computers or computer networks are used as the principal means for abusive and criminal purposes (Kaushik, 2013, p. 9). In other words, cybercrime involves the commission of a crime with the use of a computer and a computer network technology, such as the Internet. Cybercrime also includes technologically specific crimes that would not be possible without the use of computer technology as well as traditional crimes committed with the assistance of a computer (Maras, 2015). As Taylor et al. (2015) have noted, "Cybercrime has facilitated the expansion of almost every traditional crime, including drug trafficking, black market commerce, money laundering, theft, piracy, stalking, fraud, and espionage" (p. 23).

Furthermore, cybercrime is not limited by physical or geographic boundaries because of the Internet. The Internet enables cyber criminals to gain access to people, institutions, and businesses worldwide. Additionally, the Internet has increased the ease and speed with which criminal activities can be conducted. For example, billions of dollars can be stolen from a bank electronically within minutes, proprietary information and trade secrets of a business entity can be stolen electronically within a blink of an eye (Maras, 2015, p. 2).

Taylor et al. have also stated that cybercrimes include: the use of data destroying viruses that are capable of shutting down computers and the Internet by hackers, computer thieves stealing credit card and social security numbers, identity theft that has created millions of victims, theft of intellectual property ranging from trade secrets to illegal reproduction of copyrighted consumer materials, such as music and movies (Taylor et al., 2015, pp. 2-3).

Cybercrime is increasing at a rate that outstrips the rate of the measures designed to curb it. Cybercriminals have made great success in attacking and gaining access to the computer networks of both public-sector and private-sector organizations in the United States and stealing information. Some of the largest American companies that cybercriminals have successfully attacked include: Target, Home Depot, Adobe, eBay, AOL, CNET, JP Morgan, and many more. These security breaches have adversely affected millions of Americans. The attack of JP Morgan's systems resulted in the theft of information on more than 76 million American households, whereas the attack of the Target's systems resulted in the theft of names, credit card numbers, and other contact information of as many as 110 million customers. Also, a recent attack on the United States Postal Service resulted in the theft of information on almost a million employees, managers, and customers that in many cases included social security numbers of the individual victims. Identity theft can have a long-term effect on the finances and credits of its victims (cited in Bullock et al., 2016, p. 326).

Nevertheless, it is difficult to estimate the cost of cybercrime to society. In the attempt to estimate the cost of cybercrime to society, experts do conduct surveys on the cost of cybercrime to businesses and government agencies. These estimates, however, are to a great extent incorrect partly because of the numerous types of cybercrime that exist thereby making it impossible to obtain an accurate cost of cybercrime to society. It is also very difficult to estimate the monetary value on the loss of intellectual property that cybercriminals seek to steal for their own benefit. The music and movie industries report huge monetary losses on intellectual property every year (Taylor et al., 2015, pp. 8-9). By stealing intellectual property, cybercriminals benefit enormously from the high cost of investments in research and development that companies have made in their products without having to make any major capital investments themselves. Intellectual Property theft is pervasive in the music, film, software, and publishing industries. These industries depend on the sale of their licensed products to make profits from their investments. When hackers break into the computer systems that contain the master files of each of these industries or crack the codes that prevent duplication of their licensed products and sell copied or pirated versions of the products for greatly reduced prices that undercuts the intellectual property owner or agent (cf. Bullock et al., 2016, p. 327). As Kaushik has noted, "Cybercrime will make people reluctant to enter and trust the electronic world. This will hinder interchange of information between people, businesses, and governments, impacting everything from education to commerce. Therefore, we need to understand cybercrime in greater detail and take adequate protection measures so that the users feel safe online" (Kaushik, 2013, pp. xvii-xviii).

Cyber warfare

Cyber warfare involves the use of information and computer technologies as a mode of warfare to attack and destroy information and communication systems (Martin, 2015, p. 228). Cyber warfare is also known as information ware fare (Bullock et al., 2016, p. 324). Often, terrorists engage in cyber warfare by utilizing new computer technologies to disrupt and/or destroy the information and communication systems of private corporations, telecommunication companies, and government defense and non-defense agencies (Martin, 2015; Bullock et al., 2016). Conversely, cyber warfare counterterrorist activities involve the use of new computer technologies by counterterrorist agencies to intercept, compromise, and destroy terrorists' electronic activities, including their bank accounts, personal records, and other data stored in digital databases (Martin, 2015, pp. 228-229). Thus, cyber warfare involves the gathering or use of information to gain advantage over another party (Taylor et al., 2015, p. 22). Specifically, cyber warfare or information warfare involves "those actions intended to protect, exploit, corrupt, deny or destroy information or information resources in order to achieve a significant advantage, objective or victory over an adversary" (cited in Taylor et al., 2015, p. 22).

Information is one of the most important assets of both private-sector and public-sector organizations and needs to be secured. Securing information is critical to the success of every organization, and it leads to maximization of the benefits of information technology (Vacca, 2014). Information security involves the protection of information recorded, processed, stored and transmitted. As stated by Kaushik (2013), "The objective of information security is to protect the interests of those relying on information and systems, from the harm resulting from failure of availability, confidentiality and integrity" (pp. 235-236).

A cyber attack can adversely impact one or more of these three basic information security attributes collectively known as the CIA triad: confidentiality, integrity, and availability (Loukas, 2015, p. 2). The purpose of confidentiality is to ensure that information can be accessed only by those authorized to access it. The aim of integrity is to ensure that information or an information system's configuration can be modified only by persons authorized to modify it. And availability is aimed at ensuring that persons authorized to access particular information or a service can access it when necessary (Loukas, 2015, p. 2).

The consequences of information security breaches can be financially costly to an organization and detrimental to its operations as well. It can also severely damage the reputation of an organization (Vacca, 2014, pp. 9-10). Therefore, intrusion detection and prevention are critical to information security. Intrusion detection involves the process of monitoring events occurring in a computer system or network in order to be able to detect and analyze threats to the computer system or network. Intrusion prevention, on the other hand, involves a system set up, such as a firewall to actively block attacks that are intended to cause damage to the computer system or network (Vacca, 2014, p. 23).

Cyber terrorism

Cyber terrorism involves the actual or threatened use of violence by an individual or group motivated by ideological or political objectives. For the most part, the goal of cyber terrorism, like the goal of physical terrorism, is to intimidate or coerce a government and/or the citizens of the target government (Taylor et al., 2015; Martin, 2015; Maras, 2015; Bullock et al., 2016). According to Maras, "cyber terrorism is the politically, religiously, or ideologically motivated use of computers (or related technology) by an individual(s), group, or state targeting critical infrastructure with the intention of harming persons and/or damaging property in order to influence the population (or segment of the population) or cause a government to change its policies" (Maras, 2015, p. 183). Basically, cyber terrorism "connotes a convergence between terrorism and cyberspace" (Yar, 2013, p. 50). This means that the Internet provides cyber terrorists a means to launch attacks or threats against computer networks and information systems. As stated earlier, as a society's social, political, and economic dependence on the Internet continues to grow so will its vulnerability to cyber attacks – whether in the form of cyber terrorism, cybercrime, or cyber warfare – continue to grow.

Cyber terrorism poses a substantial and increasing threat to homeland security because of the advantages provided to cyber terrorists by the Internet. For example, because of the Internet, cyber terrorists no longer need to gain physical access to a target location because the target can be accessed through computers and computer networks. The Internet also acts as a force multiplier on behalf of cyber terrorists. As a consequence, cyber terrorists can maximize the impact of their attacks on a target with application of minimum human and technical resources. "A force multiplier is something that can increase the striking potential of a unit without increasing its personnel. One instance of such force multiplication is the impact of computer viruses: small pieces of malicious code can spread rapidly across the global network of the Web, reproducing exponentially and corrupting systems as they go" (Yar, 2013, p. 54).

Moreover, the Internet affords cyber terrorists the opportunity for anonymity, thereby enabling them to disguise or hide their actions. One of the greatest challenges facing law enforcement is the opportunity for anonymity provided to cyber terrorists by the Internet. It makes it difficult for law enforcement to track and identify cyber terrorists and bring them to justice. The lack of security on the Internet against cyber attacks due to the nonexistence of an effective centralized and coordinated regulatory scheme bodes well for cyber terrorists and very challenging to law enforcement ability to apprehend and prosecute them (Year, 2013). Maras contends that "For an act to be considered cyber terrorism, the target must be the critical infrastructure of a nation. The national definition for critical infrastructure varies across countries" (Maras, 2015, p. 182). According to the United State Department of Homeland Security, critical infrastructure/key resources (CIKR) refers to the assets, systems, and networks, whether, physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof (cited in Martin, 2015, p. 226). Additionally, the U.S. Department of Homeland Security has identified 18 different critical infrastructure sectors, including food and agriculture; chemical; dams; critical manufacturing; commercial facilities; communications; banking and finance; defense industrial bases; government facilities; energy; emergency services; information technology; nuclear reactors, materials, and waste; postal and shipping; transportation systems; water; healthcare and public health; national monuments and icons (cited in Maras, 2015, p. 183).

All of these critical infrastructures are equally important for homeland security because any security breach on one of them would have a debilitating effect on homeland security. Therefore, each one of them must receive equal attention and protection by authorities who have the responsibility for their protection against cyber attacks (Maras, 2015, p. 183). The section that follows takes a look at the consequences of cyber attacks on national critical infrastructure.

Consequences of Cyber Attacks on Critical National Infrastructure

The United States is perhaps the most critical infrastructure reliant nation in the world. Thus, the United States is very much at risk of critical infrastructure cyber attacks. Consequently, the U.S. is greatly concerned about cyber attacks on its critical infrastructure because of the grave consequences that such attacks would have on the national economy and the American people (Taylor et al., 2015, p. 26-29). Cyber attacks on any of the critical infrastructure systems can lead to catastrophic losses, which could include loss of movement for people and things, disruption of trade and commerce, breaks in communication across both short and long distances, a loss of power generation and transmission, inadequate access to healthcare, and much more (Bullock, et al., 2016, p. 322).

The importance of the United States' critical infrastructure to political, economic and social life in America makes them desirable targets for terrorists' attacks. Attacking the critical infrastructure systems can for the most part cause more financial damage and affect more people than attacking people or structures directly (Bullock et al., 2016, p. 322). For example, electrical power and water supply systems rely heavily on electronic sensors. Manipulation of these electronic sensors remotely by cyber terrorists can result in very serious adverse social and economic consequences to businesses and the American public. Furthermore, civil aviation can be greatly impacted by cyber attacks because of its heavy reliance on other critical infrastructure systems, such as electricity and communications systems. As an example, radar operates through telephone lines. If those telephone lines suffer cyber attacks, the impact could be catastrophic to the airline industry (Taylor, et al., 2015, p. 27).

Moreover, according to Year (2013), terrorist threats to critical infrastructure include what is termed critical information infrastructure (CII). Critical information infrastructure comprises "the information and telecommunications sector, and includes components such as telecommunications, computers/software, the Internet, satellites, fiber-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows" (cited in Year, 2013, p. 52). The totality of interconnected computers and networks is an essential element of critical infrastructure that has led to the growth of the Internet and plays an increasing central role in the political, economic and social life in the United States and other industrialized and industrializing countries. As a result, electronic communication networks are used increasing for commercial transactions (e-commerce) and banking and finance (e-banking, financial transfers, stock markets, etc.) Cyber attacks on these networks would be devastating to the welfare of the nation as disruption of the information infrastructure through viruses, worms, and so on would seriously undermine the operations of critical infrastructure (Year, 2013, p. 52).

Critical infrastructure is and will remain a primary concern for homeland security (Bullock et al., 2016, p. 322). As the United State becomes more advanced and complex, the greater its reliance on critical infrastructure to support the existence and lifestyle of the American people. Our daily activities could be interrupted, potentially for a long period of time, wreaking havoc on the nation. As stated earlier, the loss or disruption of one critical infrastructure system would have a disastrous impact on the nation as each critical infrastructure system relies on the others— with the result that – a failure in one system could lead to a cascading failure in other systems, causing even bigger problems for private sector and public sector organizations, including the American people (Taylor and Swanson, 2016, p. 287). In the next section, I discuss the strategies for achieving cyber Security.

Strategies for Achieving Cyber Security

The strategies for achieving cyber Security can be classified into two categories: 1) technical, and 2) nontechnical. The technical strategies basically involve technical mechanisms that are used to secure the cyber infrastructure of the nation. "Cyber infrastructure includes all of the information and communications systems and services; the hardware components and software systems that process, store, and communicate that information; and different combinations of these different components that are arranged in a manner as to perform one or more tasks or provide one or more services" (Bullock et al., 2016, p. 323). Cyber threats or attacks including cybercrimes, cyber warfare, and cyber terrorism occur in cyberspace, which involves cyber infrastructure systems.

According to Yar (2013, p. 3), cyberspace is the realm of computerized interactions and exchanges that seems to offer a vast range of new opportunities for criminal and deviant activities. Bullock et al. have described cyberspace as follows: "Cyberspace is a related term and refers to the global network of information technology infrastructure, inclusive of the Internet, the telecom network, systems of servers and computers, electronic control mechanisms, and the embedded processes in microchips and other semiconductors. All of this translates to a monumental area of coverage for the cyber Security function" (Bullock et al., 2016, p. 323). Therefore, it is imperative to secure the nation's cyber infrastructure in order to achieve cyber Security. The sub-section that follows provides a brief description of each of the selected technical mechanisms, out of many, that are commonly used to secure the cyber infrastructure of the nation.

Selected Technical Mechanisms for Securing Cyber Infrastructure

Cyber threats and attacks can be carried out using a myriad of cyber weapons, such as malicious websites, viruses, Trojan horses, worms, spyware, bots, phishing, spoofing, and so on (for more information on these cyber arsenal and many more, see bullock et al., 2016, pp. 330-334). However, the nation's cyber infrastructure systems can be secured from cyber threats and attacks using the following selected technical mechanisms which are briefly discussed here with information from Loukas (2015, pp. 182-211).

Firewall: Firewalls are filtering tools that act as barriers between the internal network and any other network, such as the Internet. They can be software based or hardware based. The function of firewalls is to guard the in-coming and out-going traffic of the internal network according to predefined set of criteria about what is and what is not authorized. Upon receiving a network packet, the firewall analyzes the characteristics of the network packet, such its source address, destination address, port number, network status, actual data delivered, etc., and then determines whether to let it go through, drop it, delay it, or redirect it for further inspection. Some firewalls, like state full firewalls, keep a history of the packets inspected in order to track ongoing network sessions and anticipate what subsequent legitimate packets should look like. Proxy firewalls protect users in the internal network by acting as intermediaries and establishing on behalf of the users any external connections that they require, whereas deep packet inspection firewalls take the packets apart, analyze the data contained in them, and look for particular content that would indicate a threat or an attack.

Intrusion Detection Mechanisms: Intrusion detection mechanisms are designed to detect cyber attacks on a computer system or computer network system. They are very important for securing cyber infrastructure system since it is very difficult to prevent all possible attacks against a system. Intrusion detection mechanisms can be knowledge-based, behavior-based, or a combination of both. Knowledge-based intrusion mechanisms operate by first compiling an attack dictionary, which is a database of known attacks, each showing a particular pattern of network traffic rate, sequence of function calls, sensor measurements and other characteristics that are referred to as the input features of the detection mechanism. When in operation, knowledge-based detection mechanisms monitor the current state of a system and look for known attack patterns. If an attack pattern is detected, they raise an alert and state which type of attack has been detected, usually accompanied by a level of confidence on the detection, such as low, moderate, and high. Otherwise they assume that there is no attack in progress. Knowledge-based mechanisms can be very accurate in detecting attacks because they exhibit a high probability of detecting attacks. Conversely, behavior-based intrusion mechanisms are much better at detecting attacks that have not been previously recorded. They operate by first defining what behavior should be considered as ordinary for a particular system, and then look for evidence of behavior that is out the ordinary. This makes them very suitable for securing cyber infrastructure systems.

Antimalware Mechanism: Antimalware mechanisms are designed to prevent, detect, identify, and remove malware, which is a term used to refer to malicious computer software that are designed to disrupt, compromise, or steal information from a computer system. Antimalware applications used to detect and identify and possibly remove malware commonly scan the contents of a file and compare it against a blacklist of known malware. In this manner, they are very similar to knowledge-based intrusion detection mechanisms. Nevertheless, for an antimalware application to be effective, it must always be updated. This implies some form of Internet connectivity in order to be able to download the latest malware signatures. In an industrial control system, where direct Internet connectivity on a server with access to the control network would be too risky, malware signatures may first be downloaded on an isolated computer, and then applied to the control network's computers manually.

Cryptography: Cryptography is critical in the field of cyber Security, and is the primary measure that is taken to protect confidentiality, integrity, and authenticity in modern computer and communication systems.

Cryptography is the art and science of designing ciphers, which are the algorithms used to encrypt and decrypt messages. Ciphers are also known as cryptographic systems. And all modern ciphers use keys, which are sequences of bits that determine the output of cipher. In symmetric ciphers, there is one secret key for both encryption and decryption. The cipher takes the plaintext as input and the secret key performs various substitutions and transformations over multiple steps. The output is the cipher text. To decrypt the cipher text and retrieve the plaintext, one needs to know the secret key. This introduces a significant challenge in the process since the intended recipient of a message needs to have somehow already received the secret key in a manner that cannot be intercepted by an adversary. What is interesting with symmetric cryptography in computer systems is that the exchange of the secret key can be achieved partly via physical means. This has led to new techniques that are undergoing laboratory testing.

In asymmetrical ciphers, there is a private key and a public key. Anyone can encrypt a message using the public key, which is not secret. However, only the owner of the private key, which is secret, can decrypt it. This means that the private key should never be shared. Sharing key is a significant weakness of symmetric cryptography. The downside is that asymmetric ciphers are generally much more complicated than symmetric ones, which makes them slower and less practical for large blocks of data. A common practice to get the best of both worlds is to use a symmetric cipher to encrypt the message and an asymmetric cipher to encrypt the secret key before sharing it with the intended recipient. In addition to protecting confidentiality, the concept of asymmetric cryptography can also be used to create digital signatures that verify authenticity and integrity.

Survivability Mechanisms: Survivability mechanisms are a class of protection mechanisms that are built based on the assumption that cyber attacks on cyber infrastructure systems do succeed sometimes. Ordinarily, most protection mechanisms are designed to detect and prevent cyber attacks. An attack that is detected early enough and is thwarted will probably have little impact on its target. However, because survivability mechanisms are built on the assumption that cyber attacks on the cyber infrastructure systems sometimes do succeed, they instead of or in addition to preventing cyber attacks, aim to minimize the impact of cyber attacks on a target. Thus, the goal of survivability mechanisms is survivability, which is the ability of a system to operate correctly and with minimal performance degradation even if it has suffered a successful attack which perhaps compromised parts of it. In the next sub-section, I discuss the nontechnical strategies for achieving cyber Security.

Nontechnical Strategies for Achieving Cyber Security

The nontechnical strategies for achieving cyber Security include policy-oriented measures, such as authentication and other activities/actions that stakeholders need to take in the effort to achieve cyber Security. As we have already learned, achieving cyber Security is of utmost importance in assuring homeland security. This requires cooperation and coordination of efforts on the part of all stakeholders: individuals, businesses, and governmental agencies in order to ensure that each stakeholder has the ability and capability to protect its own data, computers, and computer networks from any and all forms of cyber threat or attacks. This is very important because, as stated earlier, no matter how strong the technological protections of a system is, those technological protections can be bypassed by a hacker who is able to trick a person who has legitimate access to the system to give up login information (Bullock et al., 2016; Loukas, 2015).

Therefore, a well-developed password authentication system should be initiated and implemented since password-based authentication is often the first line of defense for computer systems, as well as for many types of cyber infrastructure systems that involve control by human users. Authentication is concerned with determining whether a subject (a user, an application, a process, or a device) should be granted access at all (Loukas, 2015, p. 188). Thus, it is absolutely necessary to adopt optimal policies for choosing passwords that are sufficiently secure, and yet not very difficult for a user to remember or type (Loukas, 2015, p. 182-183). Furthermore, it is highly recommended that authentication be done remotely because cyber infrastructure systems are highly dependent on network communications. As a consequence, "even a relatively strong password can become worthless if captured by an adversary while in transit through the network, especially if it is sent in plaintext" (cited in Loukas, 2015, p. 183).

Additionally, governmental agencies tasked with ensuring homeland security must work in cooperation and coordination in order to efficiently and effectively deal with cyber security threats against the nation. Thus, it is paramount that these agencies initiate and execute sustainable and viable cyber Security policies. "Failure to do so may result in dire consequences" (Martin, 2015, p. 226).

These agencies must also ensure that the national cyber infrastructure systems are sufficiently hardened in order to deter or prevent cyber attacks from succeeding. Thus, the homeland security agencies must invest heavily in new computer and information technologies in terms of equipment and training because new computer and information technologies make it possible for criminals and terrorists to take advantage of the opportunities – to carry out criminal and terrorist acts against public and private sector organizations – offered to them in cyber space (Martin, 2015; Taylor et al., 2015; Loukas, 2015; Kaushik, 2013; Bullock et al., 2016). Furthermore, it is very important to align cyber security efforts among individuals, private-sector organizations, and government agencies continuously as new cyber security threats will never cease to come up (Kaushik, 2013, p. 241). Cooperation is also critically important on the part of all stakeholders in the effort to build a knowledge repository on best practices and security assurance, in building a common vulnerability database, and in building common criteria for information security products (Kaushik, 2013, p. 242).

Conclusions

This article provides a detailed discussion of cyber Security for the purpose of providing information that enhances knowledge and understanding of cyber Security. The article also explored the extent to which cyber Security is essential to homeland security and found that cyber Security is to a great extent essential to homeland security. Cyber attacks are very serious and are increasingly threatening to homeland security. As stated earlier, cyber attacks by a nation, group, or individual can result in enormous social and economic damage and disruption that could jeopardize the welfare of the nation and the American people. Therefore, all stakeholders: individuals, businesses, and government agencies with the responsibility to ensure cyber Security to protect the homeland must coordinate all efforts and utilize all available resources to secure the nation's cyber infrastructure in order to protect the national critical infrastructure from cyber attacks whether in the form of cybercrime, cyber warfare, or cyber terrorism. Otherwise, the security of the nation against cyber attacks would be severely hampered. Furthermore, as noted above, the consequences of successful cyber attacks on the nation's critical infrastructure can be devastating to our daily activities and can wreak havoc to the nation. Even the loss or disruption of one critical infrastructure system would have a disastrous impact on the nation as each critical infrastructure system relies on the others. This means that a failure in one critical infrastructure system could lead to a cascading failure in other systems, causing even bigger problems for governments, businesses – big and small, and the American people. Therefore, ensuring cyber Security is critical to ensuring homeland security.

References

Bullock, Jane A., George D. Haddow and Damon P. Coppola (2016). Introduction to Homeland Security. Fifth Edition. Waltham, MA: Butterworth-Heinemann.

Department of Homeland Security. "Cyber Security Overview," at http://www.dhs.gov/cyber-security-overview, p. 1.

Department of Homeland Security. "United States Department of Homeland Security," at
http://www.bing.com/search?q=department+of+homeland+security&from=PRUSEN & m

Dwyer, Terrence P. Legal Issues in Homeland Security: U.S. Supreme Court Cases Commentary and Questions (2015). Flushing, NY: Loose leaf Law Publications, Inc.

Gaines, Larry K., and Victor E. Kappeler (2015). Policing in America. Eighth Edition. Waltham, MA: Anderson Publishing, Elsevier Inc.

Howard, Russell D., Reid L. Sawyer and Natasha E. Bajema (2009). Terrorism and Counter-Terrorism: Understanding the New Security Environment: Readings and Interpretations Third Edition. New York, NY: The McGraw-Hill Companies, Inc.

Kaushik, Anjali (2013). Sailing Safe in Cyberspace: Protect Your Identity and Data. Thousand Oaks, CA: SAGE Publications, Inc.

Kennedy, Leslie W., and Edmund F. McGarrell (Eds.), (2011). Crime and Terrorism Studies in Criminology and Criminal Justice. New York, NY: Routledge, Taylor & Francis.

Loukas, George (2015). Cyber-Physical Attacks: A Growing Invisible Threat. Waltham, MA: Butterworth-Heinemann, Elsevier, Inc.

Maras, Marie-Helen (2015). Computer Forensics: Cybercriminals, Laws, and Evidence. Second Edition. Burlington, MA: Jones & Bartlett Learning, LLC.

Martin, Gus (2015). Understanding Homeland Security. Thousand Oaks, CA: SAGE Publications, Inc.

More,Robert (2011). Cybercrime: Investigating High-Technology Computer. Second Edition. New York, NY: Routledge, Taylor & Francis.

Taylor, Robert W., and Charles R. Swanson (2016). Terrorism, Intelligence and Homeland Security. First Edition. Upper Saddle River, NJ: Pearson Education, Inc.

Taylor, Robert W., Eric J. Fritsch and John Liederbach (2015). Digital Crime and Digital Terrorism. Third Edition. Upper Saddle River, NJ: Pearson, Inc.

Vacca, John R. (2014). Managing Information Security. Second Edition. Waltham, MA: Syngress, Elsevier Inc.

Van Brunschot, Erin Gibbs, and Leslie W. Kennedy (2008). Risk Balance & Security. Thousand Oaks, CA: SAGE Publications, Inc.

White, Jonathan R. (2012). Terrorism & Homeland Security. Seventh Edition. Belmont, CA: Wadsworth, Cengage Learning.

Yar, Majid (2013). Cybercrime and Society. Second Edition. Thousand Oaks, CA: SAGE Publications, Inc.