Obamacare Cyber Perspectives: Connecting the Dots on Beneficiaries' Data Security Speculation

Daniel Udo-Akang, CGEIT, PhD
American Military University
West Virginia
111 W Congress Street
Charles Town, WV 25414, USA.

Abstract

In the past few years, governments and businesses have taken advantage of the exponential growth and interconnectivity within the cyberspace to expand their digital transactions, services, and operations. As government services are expanded within the cyberspace, new vulnerabilities are created, enabling cyber criminals to exploit public and private assets and infrastructure. Although Internet resources are not trustworthy, U.S. dependence on e-government continues to grow as defenses are failing and the impact of cyber-attacks has not diminished. However, exploitation of cyber targets by cyber criminals represents either money or is motivated by political grievances. This article is structured to provide insights about challenges and speculations regarding the security of Obamacare beneficiaries' data in the cyberspace. Although the healthcare marketplace entered the cyberspace as an attractive target for political adversaries, it could not be considered an attractive target to cyber criminals compared to high-profile networks such as credit bureaus, hospitals, DHS, department of driver services, Social Security administration, and other e-government websites. This article may create awareness on cyber security issues regarding e-government and e-transactions, contribute new knowledge to address cyber security issues, and contribute to the academic enterprise.

Keywords: Data Security**,** Obamacare**,** Cyber Attacks, Internet Exploitation, Cyber Technologies, Cyber Security, Cyber Criminals, E-government

1.0 Introduction

Information technology advancement inevitably creates institutional dependence on the capabilities of the World Wide Web. The United States of America, for example, depends largely on the Internet for homeland and national security services and the control and management of its critical infrastructure, such as power transmission and distribution, communications, financial institutions, supply chains, transportation, energy, water supply, the healthcare system, and other government services (DoD, 2011; Savage & Schneider, 2009). Unfortunately, the security of these infrastructures is a challenging endeavor because the Internet that empowers us to manage, control, create, and "also empowers those who would disrupt and destroy" (White House, 2010, p. 27). According to Clapper (2011), "the cyber environment provides unprecedented opportunities for adversaries to target the U.S. due to our reliance on information systems" (p. 26).The convenience associated with the convergence of networks also provides the opportunity for cyber warriors and criminals to infiltrate, disrupt, and exploit vulnerable processes and systems. Although the internet resources are not trustworthy, the U.S. dependence on e-government continues to grow as the defenses are failing and the impact of cyber-attacks has not diminished (Savage et al., 2009). As government services are expanded within the cyberspace, new vulnerabilities are created, enabling cyber crackers and warriors to exploit public and private assets (Clapper, 2011). In the past few years, there has been a dramatic increase in cyber-attacks targeting U.S. networks. Although the convergence of networks amplifies the opportunity for disruptive and destructive cyber-attacks across government institutions and the economy, it adds value to the administration of services (Clapper, 2011). However, it is difficult to find a network free from cyber-attacks. The Obamacare marketplace is no exception. For example, a Department of Homeland Security (DHS) official told ABC News that the department encountered 626 attacks a day in 2012 compared to 16 attacks on a high profile Obamacare website (Larotonda & Newcomb, 2013).

In recent years, cyber-attacks have gotten more sophisticated, going after government institutions, defense industries, financial institutions, critical infrastructures, and high profile businesses (Ginovsky, 2012; Mclaughlin, 2011; Nachreiner, 2013).Criticism regarding the survival of Obamacare within the cyberspace constitutes political contestation. After all, the Social Security, immigration systems, citizenship processing, financial institutions, utility billing systems, driver's licenses, medical data, insurance data, critical assets, homeland security facts, and even national security data are all within the World Wide Web – the Internet. Any new organization, business, institution or service introduced into the cyberspace must undergo strategic adjustment to ensure its functionality and survivability. Cyber rogues have successfully breached some big corporations and institutions around the world, especially organizations that rely on legacy defenses and security logs (Nachreiner, 2013). Even though software experts have offered some secure cryptographic algorithms and technologies, including standards, controls, and measures to safeguard data and information in government databases, businesses, and organizations, several tools and deceptive techniques have also been designed by cyber criminals to evade highly configured security barriers (Ginovsky, 2012).Immunity from cyber-attacks is not guaranteed for any organization or business that takes advantage of the exponential growth and interconnectedness of digital transactions and operations within the World Wide Web (Clarke, 2010; Lute, 2013). Healthcare.gov entered the cyberspace as an attractive target for political adversaries and cyber warriors. Watchguard (2013) stated, "Imagine you're a hacktivist trying to make a big political statement - what better place to capture the notice of millions? (p. 2).The Obamacare marketplace became an alluring interactive online target for cyber warriors to inflict denial of service attacks (Krawczyk, 2013; Watchguard 2013). However, attacks on the Obamacare website are not a unique phenomenon because any sort of cyber interconnected infrastructure is susceptible to hacking. This article is structured to provide insights about the challenges of cyber transactions associated with government services in relation to the Obamacare marketplace.

2.0 Literature Review

The purpose of this article is to provide a wrap up on the speculation regarding the security of Obamacare beneficiaries' information in the cyberspace. It provides thoughtful insights on the challenges of e-government services in relation to Obamacare security. The literature review is structured to provide clarifications on (a) the nature of cyber-attacks, (b) sophistication of cyber-attacks, (c) Obamacare security contestations, and (d) e-government security challenges. In addition to articulating explicit knowledge regarding financially motivated cyber threats and politically motivated threats, this article may create awareness on cyber security issues, contribute new knowledge to address cyber security issues, and contribute to the academic enterprise.

2.1 The Nature of Cyber Attacks and Techniques

Cyber-attacks are becoming increasingly sophisticated and organizations and institutions are constantly under attack despite firewalls (FW), intrusion detection systems (IDS), evasion prevention systems (EPS), anti-virus applications, network patches, *fuzzers*, and many penetration detection tools available in the cyber security marketplace (Codenomicon, 2010; Ginovsky, 2012; Mclaughlin, 2011). Although organizations have spent millions of dollars on the procurement and installation of FW, EPS, IDS, and other detection and penetration tools, devices, and software, the insecurity and untrustworthiness of Internet resources continue to provide opportunities for cyber rogues to discover flaws in the security perimeters of government institutions' networks (Bodhani, 2012). Thus, highly skilled hackers continue to conduct successful vulnerability and penetration tests to ensure accurate attacks (Bodhani, 2012). According to Kevin Mitnick, all the firewalls and encryption in the world will never stop a gifted social engineer or a *savvyskiddie* from rifling a corporate database or an irate employee determined to crash a system (cited in Mitnick & Simon, 2011). In addition, the cyber expert, Mitnick noted, "If an attacker wants to break into a system, the most effective approach is to try to exploit the weakest link – not operating systems, firewalls or encryption algorithms – but people" (cited in Thomas, 2008, p. 4).

Cyber attackers take advantage of disgruntled employees or careless Internet users by using techniques such as phishing, password cracking, social engineering, and other advanced deceptive methods to exploit network vulnerabilities or compromise their confidentiality, integrity, and availability (Udo-Akang, 2012). The growth in software technologies has also provided opportunities of accessing every activity in the cyberspace. Cyber attackers have invested substantial amounts of money, time, and resources in research, design, and development of more sophisticated evasion techniques to exploit vulnerabilities (Juuso, Kittilä, & Takanen, 2013).

Mitigation strategies against denial of service (DoS) or distributed denial of service (DDoS) used by institutions have not been able to provide in-depth safeguards against a variety of hacking tricks, zero-day vulnerabilities, and evasion techniques (Juuso, Kittilä, & Takanen, 2013; Lemos, 2012). Many institutions do not have enough protocol-decoding capabilities to manage the changing nature and sophistication of cyber threats (Lemos, 2012).

2.2Sophistication of Cyber Attacks in Online Marketplace

The growth of the Internet with numerous tools and platforms, including the development of all kinds of networks – wired, wireless, virtual, mobile, and cloud has triggered enhanced capabilities and efficiency of governments and organizations (Dzemydiene, Jasiunas, Kalinauskas, & Naujikiene, 2010). Likewise, the capabilities of cyber warriors have advanced, in sophistication, tools, and techniques (Dzemydiene et al., 2010). Yet, organizations and governments continue to rely on the cyberspace despite that their intrusion detection and prevention systems are incapable of preventing attacks in a globally interconnected network with highly skilled criminals and sophisticated cyber intrusion tools (Lute, 2013). The world's leading information technology companies, such as Apple, Microsoft, Google, America Online, and Yahoo have developed several distributed computing tools to enhance cooperative, collaborative, and interoperability of cyber rogues and users of the World Wide Web (Camelia, Cristian, & Elena, 2008).It is practically impossible to avoid cyber dependence despite advances in disruptive technologies. According to Bisson, Bughin, Chui, Dobbs, Manyika, and Mars (2013), "technology is moving so quickly, and in so many directions, that it becomes challenging to even pay attention – we are victims of "next new thing" fatique" (p. iv). Cyber technology is uniquely sophisticated and capable of providing synchronous and asynchronous interactions but it is also full of surprises, uncertainties, and threats. Cyber-attacks come in several flavors, techniques, versions, and capacities. For example, malicious actors could use tools such as: Wireshark (Rajavenkateswaran, 2012); Firesheep (Andrew, 2010); Secure Socket Layer Strip (Sarac, 2012); Eavesdropping (Man-in-the-Middle) attacks; Advance Evasion Techniques (Softstone, 2012); and Backtrack 5 to downgrade, hijack, and exploit any secured Internet sessions or transactions. It is possible for cyber warriors to use these tools to exploit any e-government services, including the Obamacare website.

As a secured and encrypted form of Hypertext Transfer Protocol, Hypertext Transfer Protocol Secured (HTTPS) directs Uniform Resource Locator (URL) connection between web browsers and web servers using Secure Socket Layer (SSL) protocol. However, cyber criminals were able to use tools such as SSLstrip based on secure hypertext transfer protocol (HTTPS) to trick internet victims into insecure web browser or HTTP connections instead of HTTPS with a secure socket layer –A Man-in-the-middle attack against SSL (Adeloye, 2013; Seifried, 2010). Adeloye (2013) discussed the possibility of cyber crackers to inject destructive code into careless downloads from Internet sites that do not either use HTTPS or use HTTPS without a strict transport security (HSTS) policy (Adeloye, 2013). In the context of the Obamacare website or any other government services within the cyberspace, the connection between customers and the marketplace is based on Secure Hypertext Transfer Protocol (HTTPS) or Insecure Hypertext Transfer Protocol (IHTTP). Secure Socket Layer (SSL) has been a widely used protocol for encryption across the Internet to secure all transactions between the Internet user and the server (Al Bawaba, 2013).

Before 2009, it became apparent that SSL has become a weak tool that an attacker could intercept, disable the connection and spy or reroute the data on transit to a malicious site (Adeloye ; Al Bawaba, 2013). Apart from the SSLstrip, the attacker could use other exploitation tools such as Firesheep as a man-in-the-middle (MITM) tool to hijack web sessions and applications that process users' identifications information through HTTPS (Adeloye, 2013; OTA, 2012). Alternatively, an attacker could eavesdrop on an MITM connection between a user and that person's destination to relay messages or data as if they were talking to each other. Tools that are available to an ethical hacker is equally available to the cyber rogues. For example, Network sniffer, such as Wireshark could be used to analyze network traffic – to identify source and destination addresses and ports, decipher payloads, and watch malware behavior (Lynn, 2008; Rajavenkateswaran, 2012). Wireshark as open source software (OSS) has the capability to identify virtually all network communication protocol including voice over Internet Protocol (VoIP) and wireless (Rajavenkateswaran, 2012). Some cyber attackers prefer to use Wireshark to capture IP addresses of high-profile targets (Lynn, 2008; Rajavenkateswaran, 2012), using NMAP to locate vulnerable ports (Wolfgang, 2002), and using Backtrack-5 to exploit and inject viruses through the open ports (Ramachandran, 2003; Tabaka, 2012). All these exploitation capabilities are associated with e-government marketplaces similar to e-businesses in conventional marketplaces.

The Internet security landscape is changing and cyber threats have grown in scale, techniques, and sophistication in recent times. Malicious websites and codes capable of compromising vulnerable computers and networks have increased significantly (Ballard, Jagpal, Mavrommatis, Nojiri, Provos, Rahab, & Schmidt, 2011). As information technology resources are developed and deployed to enhance e-government and e-business marketplaces, cyber adversaries are becoming more skilled in designing evasion techniques to cloak against scanners (Ballard et al., 2013). Ginovsky (2012 and Softstone (2012) discussed the capabilities of advanced evasion techniques (AET) as (a) the ability to circumvent standard DoS defenses and (b) the ability to bypass the security detection and logging capabilities of a particular network. Similarly, Lemos (2012) posited that hackers craft packets designed to evade IT/IS defenses of their target organizations, specifically by sending a massive influx of DoS traffic to bombard targeted sites with 70-100Gigabytes/sec of peak requests. Thus, "By crafting the data to look like valid encrypted Web requests, the network packets are allowed to get through to the customers' own computers to decipher the information. Even if that system blocks the requests as invalid, the avalanche of data buries the computer, which can't keep up" (Lemos, 2012).According to Softstone (2012), the risk stake of AET requires (a) zero-day AET protection in all layers, (b) deep packets inspection across multiple network layers and communication protocols, (c) infrastructure patch capabilities, (d) high manageability, and (e) integration capabilities. The major advantage of e-government is the ease of connectivity of the clients and the efficiency in terms of information flow regardless of geographical distance (Sarac, 2012). All e-government services such as immigration, Internal Revenue Services, Social Security, credit reporting, and Obamacare take advantage of the convenience and efficiency of cyber interconnectivity to provide services even though cyber threats are known to exist. Thus, the challenges of e-government regarding Obamacare by political actors is a generic concern applicable to all government services and processes within the World Wide Web.

2.3Obamacare Cyber Security Contestations

There have been several arguments and political contests about the survival of Obamacare within the cyberspace. Mike Rogers, Chairman of the House Intelligence Committee stated, "Americans' personal information is the subject of hundreds of thousands of hacking attempts worldwide" (CCHF, 2013, p. 1). The Congressman further noted "Every shred of data one would need to steal your identity or access your confidential credit information would be available at the fingertips of a skilled hacker, producing a staggering security threat" (CCHF, 2013, p.1). Within the information technology environment, it is arguably true that any organization with valuable data or information is subject to cyber threats of various types (Websense, 2011). As Christopher Rasmussen, a policy analyst at the Center for Democracy and Technology argued, "Any sort of interconnected [Information Technology] infrastructure is vulnerable to hacking" (Sasso, 2013).The question is what distinguishes the Social Security Administration, the driver's license bureau, the citizenship bureau, credit report websites, and other sensitive government interconnectivity with the Affordable Care Act (Obamacare) website in terms of cyber threats? Although healthcare is considered the most transaction-intense industry in the United States (Beachboard, Pumphrey, Trimmer, & Wiggins, 2006), Obamacare does not need any medical information for enrollment, other than such questions as, 'Do you smoke?"(Leithauser, 2013).As Cyber expert reported, considering that some government websites gets hundreds and thousands of cyber assaults each day, 16 reported attacks on Obamacare website is surprisingly small number (cited in Larotonda et al., 2013). For example, the Homeland Security website logged about 228, 700 cyber incidents in the last fiscal year, which was about 626 attacks per day (cited in Larotonda et al., 2013).

The basic idea about cybercriminals is that they steal data from businesses and organizations for financial gain. Healthcare data is typically spread throughout healthcare institutions and is held in incompatible and disjointed systems with little or no secure interconnectivity (Khosrowpour, Pendharktar, & Roger, 2001). Why would a cybercriminal hack into the Obamacare website to steal information from beneficiaries who had no money to buy health insurance prior to the enactment of the Affordable Healthcare Act? The only thing cyber warriors could possibly do to the Obamacare network is to threaten it with DoS attacks like they do to most networks. According to Krawczyk (2013), the Obamacare website was threatened by hackers using DDoS attacks. Krawczyk (2013) claimed a politically-charged tool circulating around the Internet called "Destroy Obama Care" must have overloaded the Obamacare website (Krawczyk, 2013). The tool's About page said: This program continually displays alternate page of the Obamacare website. It has no virus, Trojan, worms, or cookies.

The purpose is to overload the Obamacare website, to deny service to users and perhaps overload and crash the system. You can open as many copies of this program as you want. Each copy opens multiple links to the site (cited in Krawczyk, 2013).

In his study, *Forecasting malware conditions*, Van Der Molen (2013) argued that the exploitation of a target by cybercriminals represents money. Clearly, if the Obamacare website was exploited, it was politically motivated without any financial motives or an attempt to collect beneficiaries' information. Even though electronic medical record systems (EMR) are said to provide patient safety, quality of care, efficiency, ease regulatory compliance, and enhance clinical decision support (Beachboard et al., 2006), Obamacare was designed strictly as an upstream registry insurance marketplace prior to data collection at the EMR medical processing phase.

The struggle of healthcare in decision-making regarding interconnectivity in the management of beneficiaries' information is not new (Beachboard et al., 2006). While many healthcare professionals recognize the role of information technology in supporting the quality of service, others regard it as a necessary evil (Beachboard et al., 2006; Ross & Weil, 2004). However, the security of healthcare information has many dimensions. Abouzakhar (2013) discussed vulnerabilities associated with healthcare data theft, including: (a) proliferation of handheld devices, (b) interception of healthcare staff mobile communication, and (c) exploitation of poorly secured electronic patient healthcare information (ePHI) in the hospital network. Without a second thought about the Obamacare website, cyber criminals are capable of exploiting healthcare service providers who leverage the interconnectivity and distributed computing capabilities of the Internet to serve their patients without paying attention to patients' data security (Abouzakhar , 2013). The warning regarding the Obamacare network posed by the U.S. House Intelligence Committee Chairman Mike Rogers that hackers could be able to break into the hub to steal health records and other sensitive data is generic to Social Security Administration, credit bureaus, citizenship bureau, and insurance companies' networks. Arguably, the security of government services in the cyberspace is a huge challenge, including healthcare, government services, and critical infrastructure systems.

2.4E-Government Security Challenges

Just like the implementation of the Affordable Healthcare Act (Obamacare), the conduct of business activities and operations by governments and institutions all over the world have become highly dependent upon the Internet. With increasing digitization and interconnectivity of systems, assets, infrastructure, and business resources within the cyberspace, there is no "dispute regarding the importance of information security" (Cole & Spear, 2006, p. 1). Globally, Cyber-attacks is becoming more complex, frequent, and sophisticated with a capacity to disrupt and exploit critical infrastructures and key assets. In 2011, General James Clapper, the Director of National Intelligence (DNI) stated, "The national security of the United States, our economic prosperity, and the daily functioning of our government depend on a dynamic public and private information infrastructure" (Clapper, 2010, p. 26). Prior to Clapper's insight, Jim Lewis, a former State Department official, in a CBS 60 *Minutes* interview said: In 2007 we probably had our electronic Pearl Harbor. It was an espionage Pearl Harbor," Lewis said. "Some unknown foreign power, and honestly, we don't know who it is, broke into the Department of Defense, to the Department of State, the Department of Commerce, probably the Department of Energy, probably NASA. They broke into all of the high tech agencies, all of the military agencies, and downloaded terabytes of information (CBS, 2009, p. 1). Based on Clapper's and Lewis's insights, it is important for the challengers of electronic-Obamacare to understand the basic knowledge of the United States e-government interconnectivity framework.

The hospital, healthcare providers, Department of Homeland Security, Social Security and other government services, banking and finance, electrical power grid, water supply, communication, oil and gas transmission, transportation, and supply chain services are interconnected in the global cyberspace. Although each of these critical infrastructures uses a different type of network and communication protocol, cyber warriors are constantly devising techniques to circumvent all kinds of security capabilities or strip down complex communication protocols to exploit specific targets. It is the responsibility of government institutions and their external oversight authorities to develop strategies to harden their security perimeters. Although Affordable Care Act (Obamacare) website does not violate Health Insurance Portability and Accountability Act of 1996, it is also the responsibility of the Congress and the President to enact legislation to enhance the security of e-services provided by the government. According to Congressman DeGette, Democrat from Colorado, the Obamacare website would only violate HIPAA if beneficiaries were required to enter their personal medical information in the application (Leithauser, 2013).

Compared to Social Security, DHS, immigration, the driver's license bureau, insurance records, hospitals' records, credit report data, and many e-government websites, it could be argued that the Obamacare website is not an attractive target to cyber criminals. However, it could be an attractive target to the cyber warriors or cyber terrorists motivated by political or religious ideology. Nevertheless, the importance of security initiatives, strategies, mandates, and legislative tools to secure the website cannot be overstated.

Prior to the Affordable Care Act (Obamacare), the HIPAA was enacted as a broad Congressional attempt to protect the privacy and security of patient health records (Beachboard et al., 2006). The law was designed to provide a legal framework regarding the controversial electronic medical record (EMR) system and to enable the United States Department of Health and Human Services (DHHS) to develop standards for the safety of patients' medical information (Beachboard et al., 2006).Despite HIPAA and other legislation such as the Sarbanes-Oxley Act (SOX) of 2002, the Gramm-Leach-Bliley Act of 2001, and California 1386 design to protect the privacy and confidentiality of customer data (Cole et al., 2006), many technologies emerged and were implemented that undermine data management before security responses are put in place (Mishory, 2012). According to James Clapper, U.S. Director of National Intelligence, "cyber threats pose a critical national and economic security concern due to the continued advances in…and growing dependency on the information technology (IT) that underpins nearly all aspects of modern society" (cited in Mishory, 2012, p. 1). Accordingly, market incentives intertwined with functionality in technology innovation are outpacing innovation in security, such that neither the public nor private sector is capable of successfully implementing security countermeasures to harden its infrastructures or assets (Mishory, 2012).

The security of infrastructure and assets in the private and public sectors of many countries is one the most disturbing national security issues. It is the responsibility of any government to develop capabilities to secure its people, infrastructure, and homeland. In his presentation to the House Armed Services Committee, General Keith Alexander, Chief of U.S. Cyber Command, warned that the U.S. military network is under constant attack and is probed at least 250,000 times an hour (cited in Mat, 1010). He cited an instance in 2006 when 10 to 20 terabytes of information in the Non-classified Internet Protocol (IP) Router Network (NIPRnet) was ex-filtrated by cyber intruders (cited in Mat, 2010). In a similar vein, Senator Dianne Feinstein, Chairman of the Senate Intelligence Committee argued that hackers have the capability to intrude on the U.S. infrastructure to the extent of taking down a dam or an electric grid (Cited in Mishory, 2012). Recently, Leon Paneta, former U.S. Defense Secretary, warned that investment in cyber capabilities was an important step to be able to protect the nation's critical infrastructure against imminent and destructive cyber-attacks (cited in McCarthy, 2013). The former Pentagon chief noted, "Cyber-attack is now at a point where the technology is there to cripple a country, take down our power grid system, to take down our government system, take down our financial system and literally paralyze the country" (cited in McCarthy, 2013, p. 1). The Chief of the U.S. Cyber Command, General Alexander argued that the need to develop dynamic, rather than static defenses to neutralize network adversaries cannot be overemphasized (cited in Mat, 2010). The sophistication of cyber-attacks is advancing at a rapid pace. There are vulnerabilities and flaws in software and software component in hardware, which provide opportunities for cyber rogues to exploit any network, including all critical infrastructures connected to the livelihood of all American people.

3.0 Cyber Threats and Strategic Countermeasures

In his presentation at the European Conference on Information Warfare, Abouzakhar's (2013) insights supported the warnings offered by Secretary Paneta, Senator Feinstein, and General Alexander regarding the severity and sophistication of cyber-attacks. According to Abouzakhar (2013), sophistication in cyber threats and malicious activities will continue to increase due to lack of knowledge about cyber security threats and lack of proper security measures and policies. Congressman James Langevin asked the U.S. Cyber Chief, "Could you defend the nation against a major cyber-attack?" General Alexander replied: It's not my mission to defend the nation against a major threat…Our mission in Cyber Command is to defend the Defense Department networks. If we are tasked by either the secretary of Defense or the President to defend those non-military networks, then we'd have to put in place the capabilities to do so. Today we could not (cited in Mat, 2010, p. 1).

Unfortunately, cyber threats and attacks are unlikely to stop because it is cheap and unanimously conducted. All you need for an attack is a computer, an Internet connection, time, patience and, according to Chinese cyber experts at the Academy of Military Science, the Chinese have plenty of all four (cited in Ehrenfeld & Jensen, 2013).

In adhering to Sun-Tzu's *Art of War*, a cyber expert, Wang Xiadong posited, "Since thousands of personal computers can be linked up to perform a common operation … an Information Warfare victory will very likely be determined by which side can mobilize the most computer experts" (cited in Ehrenfeld & Jensen, 2013).

In all e-government services, such as Obamacare, the Social Security Administration, the Department of Homeland Security (DHS), the driver's license bureau, the IRS, and the bureau of citizenship, network vulnerabilities are created during software design, implementation, and operations. Cyber criminals exploit known and unknown vulnerabilities created by individuals involved in organization's network acquisition and management. In the cyberspace, every material or human resource used for interconnecting assets and infrastructures is a potential threat. The cyber rogues are continuously probing the Internet using techniques such as social engineering, backdoors, phishing, logical evasion, password cracking, and several deceptive and intrusion techniques to exploit networks and compromise their confidentiality, integrity, and availability (Udo-Akang, 2012). Although sophisticated firewalls, intrusion detection systems, and various anti-virus tools have been developed and deployed to repel cyber-attacks, they do not prevent all attacks (Mclaughlin, 2011). In their research, Kapoor, Pandya, and Sherif (2011) posited that the security of data in storage, processing, and transition is based on seven security pillars: (a) authentication, (b) authorization, (c) privacy, (d) integrity, (e) non-repudiation, (f) availability, and (g) audit. The seven pillars constitute access control mechanisms, a web of trust used to protect systems and data from unauthorized access, modification, and disclosure. According to Winkel (2007), reliability and trustworthiness in the virtual world of the Internet based on the dimensions of confidentiality, integrity, and availability requires the cooperation of all varied stakeholders. Integrity represents unadulterated transmission of information, confidentiality signifies that information is only accessible to designated partners, and availability is an indication that authorized persons can make use of unadulterated information as needed (Winkel, 2007).

As cryptographic algorithms such as DES, AES, Mcrypt, symmetric key, public key algorithms, SHA-1, SHA 256, MD5, and Rivest Shamir Adleman (RSA) are introduced, cyber-attacks and techniques continue to get more sophisticated (Schneier, 2005).In the 20thcentury, data encryption was particularly confidentiality-specific, but the advent of modern encryption algorithms such as IBM's MARS, RSA Lab RC6,3DES, Serpent, Counterpane's Twofish, and Advanced Encryption Standard (AES) has provided capability to include information integrity, sender and receiver identity authentication, digital signatures, and secure interactive and computation certifications (Pfleeger & Pfleeger, 2007). Even though encryption tool kits comprise a large library of algorithms, government and high-profile businesses preferred AES as a more efficient successor to the triple data encryption standard (3DES) because of its performance, efficiency, ease of implementation, flexibility, and combination of security (Brown & Stallings, 2008; Harrison, 2000).However, cryptology is not the only tool for electronic security even though its technological value is significant in addressing security concerns and the growth of electronic commerce regarding users' authentication of transactions (Blain, 2000; Hanson, 2009). The proliferation of computer software, networks, and the Internet creates new threats and vulnerabilities, making cyber security broad and diverse. It is common practice that when software flaws become public, the vendor creates patches to correct the flaws and prevent exploitation (Brykczynski & Small, 2003). For all e-services, including the Obamacare network, data security requires proactive detection, prevention, and response (Brown et al., 2008).

Due to frequent reports of increased vulnerability and compromised systems, Brykczynski et al. (2003) suggested immediate improvement in patch management practices. Such practices involve a periodic change of the operating system to install new software releases or patches because most successful attacks take advantage of vulnerable systems for which patches have not been available prior to the attack (Arbaugh, Fithen, & McHugh, 2000). The Software Productivity Consortium recommended four cyber defense improvement methods(a) network reconnaissance; (b) system and application hardening; (c) security patch management; and (d) tools against malicious software essential and critical to e-government and e-business information security posture (cited in Brykczynski et al., 2003). According to CERT Coordination Center, effectiveness in installing patches in a timely and coordinated fashion could eliminate vulnerabilities, prevent successful attacks, promote management, and balance the need for security (Cited in Brykczynski et al., 2003). However, Brykczynski et al. (2003) presented a challenging issue, "In practice, therefore, an organization needs to focus on vulnerability management because the problem exists before the patch is published" (p. 50). The need for effective patch management reflected in the U.S. National Cyber Security Strategy issued by President George Bush's administration (White House, 2003).

According to President Bush, a majority of security vulnerabilities could be mitigated if good security practices incorporate patch selection, determination of patch suitability, and regular patching (White House, 2003). Apart from patching, many intrusion detection systems (IDS) and evasion prevention systems (EPS) have been developed to manage various cyber risks associated with advanced evasion techniques (AETs), zero-day exploitation, and other advanced persistent threats (APTs) (Codenomicon, 2010; NewsRx, 2012). Such detection tools include Evader 2.01 evasion testing device, Fuzzers that identify zero-day vulnerabilities, advanced firewall manager (AFM) for network security against widely deployed protocols such as Simple Mail Transfer Protocol, Domain Names Service, File Transfer Protocols, and Hypertext Transfer Protocols.

The Domain Name System (DNS) used in countless applications on the Internet including the Obamacare network is a critical component underlying the structure of the internet and has many security holes that enable disruption and exploitation (Hanson, 2009). DNS disruptions are not limited to re-routing of e-mails or files on the Internet, accessing of confidential medical records, accessing of electronic financial transactions between businesses; but also cache poisoning, spoofing, amplification, and hijacking of legitimate navigated webpage to a mimic malicious homepage for exploitation (Gilmer, 2013; Hanson, 2009; Kim, 2013; Nachreiner, 2013; Savvas, 2007). Due to serious consequences of these DNS disruptions, DNS security extensions (DNSSEC) was proposed for development as "a collection of 'fixes' that would close many security holes within DNS" (Hanson, 2009, p. 26).Unfortunately, the implementation of DNSSEC could require a shutdown of the global Internet or the creation of fragmented regional networks that would be unable to communicate with each other (Hanson, 2009). Such Internet fragmentation could undermine the global construct, interoperability, and functionality of the Internet (ICANN, 2008). In an effort to resolve the threat of DNS exploitation, public key cryptography was introduced to avoid shutting down access to entire Internet domains or creating demarcation lines between regional fragmented internets. Public key cryptography is an asymmetric means in which a sender securely encrypts a message to a receiver using the receiver's public key and the recipient decrypts the message using a private key (Huston, 2006; Moore, 2005). Although the public and private keys are mathematically related, it is practically impossible to construct one from another. Their relatedness is based on their logical usage in such a way that "only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them" (Moore, 2005, p. 17).

The use of these logical computations to design a security framework for a particular network and users depends largely on the value of transmitted messages, the ability to manage cryptographic keys (Efosa, 2004), volume of data, and expense label (Luther, 2007). Luther's assessment of HIPAA security standards considered these dependencies, especially the difficulty of encrypting and decrypting cumbersome health data, as inappropriate security measure for personal identifiable medical information. Arguably, HIPAA data is more complicated, valuable, and sensitive than Obamacare beneficiaries' information or other e-government services. Despite enormous efforts made by the U.S. Department of Health and Human Services regarding HIPAA privacy and data security rules, including rules for protected health information (PHI) breaches (Fensholt & Holloway, 2013), data security is still a major issue regarding HIPAA security compliance. As stated, the Obamacare enrollment website was not designed to collect any personal medical information that could violate HIPAA privacy provisions. Although legislative measures are necessary to protect federal government websites from cyber security threats and attacks, there is no justification in comparing the recent data breach or vulnerability at Target Corporation to Healthcare.gov security deliberations as portrayed by Congresswoman Candice Miller (Miller, 2014). As Van Der Molen's (2013) study posited, exploitation of targets by cyber criminals represents money. Clearly, the Obamacare website could not be considered an attractive target nor contain juicy or attractive data to cyber criminals. However, the importance of designing a competitive security framework for the Obamacare website and e-government services cannot be overstated. Certainly, it is not just one-time security implementation that makes an organization secure, but it is an ongoing investment based on the trend of cyber-attacks.

4.0 Summary

Network security is a crucial global challenge. The continued development and implementation of e-government services have been challenged by emerging threats to the confidentiality, integrity, and availability of data in storage, processing, and transit. There are many sources of danger within the cyberspace, including viruses, worm, malicious hijack, data corruption, denial or distributed denial of service, DNS spoofing or amplification, evasion attacks, phishing, brute force attacks, and many other hacking tricks. The threat environment has grown in scale, technique, and sophistication due to destructive software proliferation in the Internet (Winkel, 2007).

Businesses and online services offered by the government have been caught off-guard due to advancement and sophistication of cyber techniques and the frequency of attacks. As Digital Trend indicated in their post, "Obamacare website threatened by hackers using DDOS attacks" (Krawczyk, 2013, p. 1), and a politically-charged code "Destroy Obama Care" was developed and circulated with the aim of directing Internet traffic to overload the Obamacare website (Krawczyk, 2013). Denial of service (DOS) or distributed denial of service (DDOS) is always a politically motivated attack on high profile institutions and has nothing to do with data exploitation or stealing, as Congressman Mike Rogers argued regarding Obamacare website. However, Roger's argument that "you cannot expose this much information with this low threshold of security in a day when there are 1.5 million people ripped off every day in the cyberspace" (Leithauser, 2013, p. 2), could be applicable to networks with financial data or critical information. As Van Der Molen's (2013) study posited, the exploitation of targets by cyber criminals represents money and the Obamacare website could not be considered an attractive target nor contain juicy or attractive data to cyber criminals. The Affordable Care Act website does not require beneficiaries' medical information for enrolment other than questions like "Do you smoke?"(Leithauser, 2013).Arguably, such information is of no value to cyber criminals, whereas there is personal identifiable information (PII) available in high profile hospitals, credit bureaus, DHS, driver's license bureau, Social Security Administration, and other e-government websites.

Regarding the Obamacare network security, it could be argued that it is not just a one-time security implementation that ensures an organization's network security but continuous refinement of techniques based on emerging trends of cyber threats and attacks. By now, cyber threats regarding every e-business, e-transaction, e-service, and e-government service should be calculated into the overall organizational risk factor. For a long time, cyber threats have been in the media spotlight. Governments and businesses have expressed frustration with the sophistication of attacks. The capabilities of cyber criminals, cyber rogues, and cyber warriors have grown in recent times to show that they are capable of stripping a secured socket layer, hijacking unsecured HTTP, using AET to circumvent security perimeter, redirecting internet traffic, exploiting unidentified zero-day vulnerabilities, and decoding proprietary protocols. Cyber security is a problem for all businesses and governments because cyber criminals are capable of circumventing, overwhelming, and manipulating organizational defenses. Some attackers are capable of decrypting high level encryptions with ease. They have the capability of generating huge amounts of malicious charged code or traffic greater than an organization's network traffic can handle (denial of service). According to Lemos (2012), DDOS mitigation is no longer a cure-all cyber defense strategy unless organizations have enough protocol decoding capabilities. Otherwise, modern AETs are capable of blinding or inhibiting monitoring devices, systems, and logs (Ginovsky, 2012). The security landscape has changed. Every network, including the Obamacare network is vulnerable. As DHS official told ABCNews, the Homeland Security websites logged about 228,700 cyber incidents in the last fiscal year, about 626 a day (cited in Larotonda et al., 2013). Thus, 16 reported attacks on the healthcare.gov website is comparatively a small number. However, the exploitation of networks by cyber warriors or cyber criminals are either politically or financially motivated. The healthcare.gov website entered the cyberspace as an alluring and attractive target that enticed political adversaries to inflict their grievances on the administration.

References

Abouzakhar, N. (2013). *Critical infrastructure cybersecurity: A review of recent threats and violations.*Proceedings of the European Conference on Informations Warfare, Jyväskylä, Finland. Retrieved from http://connection.ebscohost.com/c/articles/88849584/critical-infrastructure-cybersecurity-review-recent-threats-violations

Adeloye, B. (2013). *HTTP Man-in-the-middle code execution*. Retrieved from https://ritdml.rit.edu/bitstream/handle/1850/16646/BAdeloyeThesis5-30-2013.pdf?sequence=1

AL Bawaba. (2013). *Doubts cast over mega security*. Computer News Middle East.Retrieved from Proquest.(Publication No 1271989535).

Andrew, G. (2010). Fighting sidejacking.*eWeek, 27*, 38. Retrieved from ProQuest.(Publication No 814372864).

Arbaugh, W., Fithen, W., McHugh, J. (2000).Windows vulnerability: A case study analysis.*Computer, 33*, 52-59.

Ballard, L., Jagpal, N., Mavrommatis, P.,Nojiri, D.,Provos,N., Rahab, M. A., & Schmidt, L. (2011). Trends in circumventing web-malware detection.*Google Technical Report, 2011a*, 1-12

Beachboard, J., Pumphrey, L., Trimmer, K., & Wiggins, C. (2006).*Entrepreneurial governance in a rural family practice residency program.*Proceedings of the 39th International Conference on System Sciences, Hawaii, United States.

Bisson, P., Bughin, J., Chui, M., Dobbs, R., Manyika, J., Marrs, A., Michael, J. (2013).*Disruptive technologies: Advances that will transform life, business, and the global economy.*McKinsey Global Institute. Retrieved from http://www.mckinsey.com/insights/business_technology/disruptive_technologies

Blain, C. M. (2000).*Cryptography and electronic commerce: The role of the Canadian government in facilitating a domestic and global electronic marketplace*.Retrieved from ProQuest, (Publication No MQ52340).

Bodhani, A. (2012). Ethical hacking.Bad in a good way.*Engineering & Technology Magazine, 7*, 1. Retrieved from http://eandt.theiet.org/magazine/2012/12/bad-in-a-good-way.cfm

Boyer, B. R. (2011).*Identification and ranking of critical assets within an electrical grid under threat of cyber- attack*. ProQuest Document No 1500336.

Brown, L., & Stallings, W. (2008).*Computer security*.New York, NY: Prentice Hall.

Brykczynski, B., & Small, R. A. (2003).Reducing internet-based intrusions: Effective security patch management.*IEEE Computer Security, 20*, 50-57. doi: 10.1109/MS.2003.1159029

CBS. (2009). *Cyber War: Sabotaging the System CBS 60 Minutes interview describing unauthorized terabyte download*. Retrieved fromhttp://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565_page2.shtml?tag=contentMain;contentBody

CCHF. (2013). *As online Obamacare enrollment fails, 'Glitches' endanger personal data*. Citizen Council for Health Freedom. Retrieved from http://www.cchfreedom.org/cchf.php/820

Camelia, V., Elena, E., & Cristian, M. (2008).Digital marketing – An opportunity for the modern business communication.*Annals of the University of Oradea, Economic Science Series, 17, 982.*

Clarke, R. A., &Knake, R. K. (2010).*Cyberwar: The next threat to national security and what to do about it*. New York, NY: HarperCollins.

Clapper, J. (2011).*Statement for the record on the worldwide threat assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence*. Retrieved from http://www.odni.gov/testimonies.htm

Codenomicon (2010).*Fussing best practices: Combining generation and mutation-based fuzzing*. Retrieved from http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-generation-and-mutation.pdf

Cole, R. J., & Spears, J. L. (2006).*A preliminary investigation of the impact of the Sarbanes-Oxley Act on information security.*Proceedings of the 39th International Conference on System Sciences. Hawaii, United States of America.

Cronkrite, M;Park, J;&Szydlik, J. (2011, March). The strategies for critical cyber infrastructure (CCI) protection by enhancing software assurance.*International Conference on Information Warfare and Security*, 68. Retrieved from http://connection.ebscohost.com/c/articles/60146009/strategies-critical-cyber-infrastructure-cci-protection-by-enhancing-software-assurance

DoD. (2011). Department of defense strategy for operating in cyberspace. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf

Dzemydiene, D; Jasiunas, E; Kalinauskas, M; &Naujikiene, R. (2010). Evaluation of security disturbance risks electronic financial payment systems. *Intellectual Economics, 2*, 21-29.

Efosa, O. (2004). *Encryption key management strategy*.Retrieved from ProQuest.(Publication No 3136119).

Ehrenfeld, R., & Jensen, K.(2013). *Cyber Insecurity.American Center for Democracy*. Retrieved fromhttp://econwarfare.org/cyber-insecurity/

Gilmer, B. (2013). Cyber attack. *Broadcast Engineering, 55.5*, 16-19.Retrieved from ProQuest.(Publication No 1428252205).

Ginovsky, J. (2012). Cyber threat.*American Bankers Association Journal, 104*, 24-28.

Google. (2012). How many malicious sites does Google discover every day? *CIO Insights, 15350096*. Retrieved from http://www.cioinsight.com/security/how-many-malicious-sites-does-google-discover-every-day/

Fensholt, E., & Holloway, M. (2013). HHS finalizes HIPAA privacy and data security rules, including stricter rules for breaches of unsecured PHI. *Benefit Law Journal, 26*, 95-102.

Hanson, E. (2009). *A network of nations: Why effective cybersecurity requires international collaboration.*Retrieved from ProQuest.(Publication No 1470408).

Harrison, A. (2000). Advanced encryption standard.*Computerworld,34*, 57. Retrieved from ProQuest.(Publication No216074287).

Huston, G. (2006). The theory. Internet Societyunder "The ISP Column," Retrieved from http://isoc.org/wp/ispcolumn/?cat=44

ICANN.(2008). ICANN proposal to DNSSEC-Sign the root zone. Retrieved from http://www.ntia.doc.gov/DNS/ICANNDNSSECProposal.pdf

Jansson, K., &Solms, R. V. (2013).Phishing for phishing awareness.*Behavior& Information Technology, 32*, 584-593.doi: 10.1080/0144929X.2011.632650.

Juuso, A, Kittila, K, &Takanen, A. (2013).*Proactive cyber defense: Understanding and testing for advanced persistent threats (APTs)*.12th European Conference on Information Warfare and Security. Retrieved from http://academic-conferences.org/eciw/eciw2013/eciw13-proceedings.htm

Kapoor, B., Pandya, P., & Sherif, J. S. (2011).Cryptography: A pillar for privacy, integrity, and authenticity of data communication.*Kybernetes, 40*, 1422-1439.doi: 10.1108/03684921111169468

Khosrowpour, M., Pendharktar, P. C., & Roger, J. A. (2001).Developing and testing of an instrument for measuring the user evaluations of information technology in healthcare. *Journal of Computer Information Systems, 41*, 84-90.

Kim, B. K. (2013). Methods of detecting DNS flooding attack according to characteristics of type of attacks. *Electronics And Telecommunications Research Institute*. Publication No US20130031626 A1. Retrieved from http://www.google.com/patents/US20130031626

Krawczyk, K. (2013). Obamacare website threatened by hackers using DDOS attacks.DigitalTrends.Retrived fromhttp://www.digitaltrends.com/computing/obamacare-website-threatened-hackers-using-ddos-attacks/#!zHop4

Larotonda, M., & Newcomb, A. (2013).*Obamacare website targeted about 16 times by cyber attacks*. ABCNews. Retrieved from http://abcnews.go.com/Politics/obamacare-website-targeted-16-times-cyber-attacks-official/story?id=20878814

Leithauser, T. (2013).*House Republican question security of Obamacare insurance websites*.Cybersecurity Policy Report.1. Retrieved from ProQuest.(Publication No 1461705842).

Lemos, R. (2013). *More banks come under denial-of-attack*. Retrieved from http://www.eweek.com/security/more-banks-come-under-denial-of-service-attack/

Lute, J. H. (2013).DHS Cybersecurity: Roles and responsibilities to protect the nation's critical infrastructure.*Testimony Before the House Committee on Homeland security*. Retrieved from http://docs.house.gov/meetings/HM/HM00/20130313/100390/HHRG-113-HM00-Wstate-LuteJ-20130313.pdf

Luter, M. (2007).Keys of encryption: Today's encryption technology can be cheaper, simpler, and safer. *Health Management Technology, 28*, 18-20.

Lynn, S. (2008). *Wireshark version 1.0.2 – Wireshark attacks network issues*. CRN Tech, 20.Retrieved from ProQuest.(Publication No 227603809).

Marsan, C. D. (2008). Morris worm turns 20. *Network World, 25*, 10.

Mat, W. (2010). U.S. faces many cyber threats, Commander warns. *Defense News, 23*.Retrieved from ProQuest.(Publication No 757185425).

McLaughlin, K. L. (2011). Cyber attack!Is counter attack warranted? Information Security Journal: A Global Perspectives, 20, 58-64. doi: 10.1080/19393555.2010.544705

McCarthy, M. (2013).Paneta warns of cyber threats as he readies to leave office. *Defense Daily, 257.25*.Retrieved from ProQuest.(Publication No 1314403790).

Miller, C. (2014). *Concerns mount over the security of the Obamacare website*. Federal Information & News Dispatch.Retrived from ProQuest.(Publication No 1473896333).

Mishory, J. (2012). Clapper: Cyber threats on rise as adversaries plunger tech data. *Inside the Pentagon, 28.5*, 5.Retrieved from ProQuest.(Publication No 919371475).

Mitnick, K. D., & Simon, W. L. (2011*).The Art of deception: controlling the human element of security*.Indianapolis, IN: John Wiley Publishing.

Moore, F. (2005).Data encryption strategies.*Computer Technology Review, 25*, 1-26.

Nachreiner, C. (2013, June). Attack of the network traffic: Understanding and avoiding distributed denial of service (DDoS) attacks. *Security Technology Executive*.36-38.

Pfleeger, C. P., &Pfleeger, S. L. (2007).*Security in computing*.Boston, MA: Pearson Education.

Rajavenkateswaran, V. P. (2012). *Wireshark extension for simultaneous monitoring of multiple networks.*Retrieved from ProQuest.(Publication No 1516515).

Ramachandran, V. (2011).*Backtrack 5 wireless penetration testing*. Birmingham, UK: Packt Publishing.

Ross, J. W., & Weill, P. (2004).*IT governance: How top performers manage IT decision rights for superior results*. Boston, MA: Harvard Business School Press.

Rotchanakitumnuai, S., &Speece, M. (2009). Modeling electronic service acceptance of an e-securities trading system. *Industrial Management & Data Systems, 109*, 1069-1084. doi10.1108/02635570010991300

NewsRx. (2012). Stonesoft introduces industry's first evasion prevention system EPS to mitigate the threat of advanced evasion techniques AETs. *Computer Weekly News, 3*, 316.

Sarac, M. (2012). Safety of e-business applications in serbia: Applied knowledge based on SSL traffic. *Journal of Internet Banking and Commerce, 17*, 1-18.

Sasso, B. (2013). *House Intel chairman warns ObamaCare system vulnerable to hackers*. Retrieved from http://thehill.com/blogs/hillicon-valley/technology/327309-house-intel-chairman-warns-obamacare-system-vulnerable-to-hackers

Savage, S., & Schneider, F. B. (2009).*Security is not a commodity: The road forward for cyber security research.*Computing Research Initiatives for the 21st Century, Computing Community Consortium. Retrieved from http://www.cra.org/ccc/initiatives

Savvas, A. (2007). Domain servers still a security risk. *Computer Weekly, 27*, 16.Retrieved from ProQuest.(Publication No237032488).

Schneier, B. (2005). Attacks on cryptographic hashes in internet protocols. Retrieved from http://tools.ietf.org/search/rfc4270

Seifried, K. (2010). Attacks against SSL.Retrieved from www.linuxpromagazine.com/content/download/.../060-061_kurt.pdf

Softstone.(2012). Protection against advanced evasion techniques in Stonesoft IPS. Retrieved from http://aet.stonesoft.com/assets/files/AET_Whitepaper2012-01-12_v3.pdf

Tabaka, G. (2012). The guide to backtrack.*Haking on Demand, 1*, 8-92.

Thomas, T. L. (2008). Cyberskepticism: The minds firewall. *I-Sphere*. 4-8. Retrieved from http://fmso.leavenworth.army.mil/documents/cyberskepticism.pdf

Udo-Akang, D. (2012).*Cyber attacks: Contemporary warfare*. Israel Homeland Security.Retrieved from http://i-hls.com/2013/02/cyber-attacks-contemporary-warfare/

Van Der Molen, H. (2013). Forecasting malware conditions: Worsening conditions, some bright spots.*Information Security Journal: A Global Perspectives, 21,* 269-279.doi: 10.1080/19393555.2012.694980

Watchguard. (2013). *Hackers harass U.S. healthcare hangout. The U.S. Healthcare.gov site will suffer a data breach*. WatchGuard Technologies.2014 Security Predictions. Retrieved from http://watchguard.com/predictions/papers/paper3.asp

Websense. (2011). *Advanced persistent threats and other advanced attacks. Threat analysis and defensestrategies for SMB, mid-size, and enterprise organizations.*Retrieved from https://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf

White House.(2003). The National Strategy to Secure Cyberspace. Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Winkel, O. (2007). Electronic government and network security: A viewpoint.*Transforming Government, People, Process and Policy, 1*, 220-229.doi: 10.1108/17506160710778068

Wolfgang, M. (2002).Host discovery with nmap. Retrieved from http://nmap.org/book/man-host-discovery.html