Cybersecurity in the 21st Century: Applying Cyber Threat Intelligence

Charles E. Wilson
University of Detroit Mercy

Author Note

Correspondence concerning this paper should be addressed to
Associate Professor Charles E. Wilson
Department of Criminal Justice Studies
And
Center for Cyber Security and Intelligence Studies
University of Detroit Mercy
Detroit. MI 48226
Contact: wilsonce@udmercy.edu

Abstract - In the twenty-first century, the prevention of cyber attacks on critical infrastructure, key assets, and public/private sector enterprises will become a more important element of national and international security. This paper examines the extant literature published on the increasing need for a more robust, comprehensive and proactive approach to cybersecurity. Specifically, the paper explores the contemporary cyberspace environment and the current cyber threat landscape. The paper recommends the application of cyber threat intelligence (CTI) complemented by predictive analytics as an effective method for countering cyber attacks. The purpose of the paper is to advance the knowledge in this critical area, to increase the understanding of available methods for proactive detection of network security intrusions, and to highlight an emerging innovative approach to cyber threat intelligence

Keywords*: Cybersecurity, cyber threat intelligence, network defense, and predictive analysis*

"Know thy enemy and known thyself, and you will not be imperiled in a hundred battles"

- Sun Tzu, The Art of War

INTRODUCTION

This paper is based on an extensive literature review of cybersecurity research documents and cyber threat journalism, white papers and practical assessment reports produced by subject matter experts, and open source documents, such as government reports. The paper proposes that the combination of cyber threat intelligence and predictive analytic techniques are extremely suited to be proactive core applications for improving cybersecurity defenses in all organizations operating in the cyberspace environment.

Cyber threat intelligence (CTI) is threat intelligence related to computers, networks and information technology (Farnham, 2013). The effective use of cyber threat intelligence must become an essential component of an organization's cybersecurity and network defense program. Recent cyber attacks and the ever increasing threat experience indicates that all organizations now need to focus on putting in place the fundamentals of cyber intelligence management to gain real value from threat intelligence (KPMG, 2013).

Predictive analytics is an area of data mining that deals with extracting information from data and using it to predict trends and behavior patterns. Often the unknown event of interest is in the future, but predictive analytics can be applied to any type of unknown whether it is in the past, present or future (Siegel, 2013). The core of predictive analytics relies on capturing relationships between explanatory variables and the predicted variables from past occurrences, and exploiting them to predict the unknown outcome. It is important to note, however, that the accuracy and utility of results will depend greatly on the level of data analysis and the quality of assumptions (Oracle, 2010).

The existing literature indicates that the increased frequency, sophistication, and severity of cyberattacks on individual citizens, government entities and private

sector enterprises have had a significant negative impact in many key areas, such as economic prosperity, national defense, global commerce, and homeland security. Over the past four decades, cyber attacks has evolved from a peripheral concern of minor status to a major national and international phenomenon recognized as having the potential to cause serious damage and irreparable harm to critical infrastructure and key information technology systems. The costs associated with the ever increasing numbers of severe cyber attacks are growing to levels of epic proportions in terms of threats to national security, increasing financial loss, detrimental geopolitical affairs, and interference with global commerce and trade.

In 2014, the Verizon Data Breach Investigations Report stated that there were over 63,000 incidents reported across 95 countries. Moreover, a longitudinal analysis of cyber threat descriptions (Mezzour, Carley, & Carly, 2014a) noted that there were more than 12,400 cyber threats detected by Symantec's antivirus products and over 2,700 attacks detected by their intrusion protection system. The severity of successful cyber attacks and their damaging effects are getting much worse with each passing year and this trend is predicted to continue into the future (Trend Micro Incorporated, 2013).

This paper will focus on providing a better understanding of the cyber threat landscape. Also, the paper suggests that there is a growing need for all entities operating in the cyberspace environment to adopt and implement a cyber preparedness strategy. One practical solution is the creation and implementation of the cyber threat intelligence approach complemented with predictive analytics techniques.

Researchers have shown that countries with large computing networks and monetary resources suffer an excessive number of cyber attacks (Mezzour, Carley, & Carley 2014b).

Because the United States is often cited as the most likely target for cyber attacks the paper will focus its examination, analysis, and content on cyber attacks striking U.S. targets. However, this does not diminish the appreciation and understanding of the global impact of the cyber threat phenomenon. Moreover, it should be noted

that the contemporary cyber threat problem is international in nature, scope, and magnitude.

The paper is organized as follows. The first section provides background on the scope and nature of cyber threat. The second section examines the U.S. Government assessment of the mounting cyber threat. The third section discusses the U.S. response to the contemporary cyber threat and its future actions aimed at countering this threat. The fourth section describes the application of cyber threat intelligence and predictive analytics as effective counter measures and as proactive cybersecurity defensive techniques. The final section concludes with strong recommendations, based on the evidence presented, that all enterprises operating in the cyber space environment must adopt and implement a cyber threat intelligence approach complemented with predictive analytics as the foundation of their cybersecurity strategy.

SCOPE AND NATURE OF CYBER THREATS

Cyber attacks can have crippling effects on their targets. Today, the successful cyber attackers use a combination of social engineering, malware, and backdoor activities to gain access to vulnerable computer systems. Targeted attacks or what have come to be known as "advanced persistent threats" (APTs) have proven to be an extremely successful method for gaining unauthorized entry to key computer networks and information technology systems. APT actors, by their nature, attempt intrusion after intrusion, adjusting their operations based on the success or failure of each attempt. At a strategic level, analyzing multiple intrusion events over time will identify commonalities and overlapping indicators. The nature of the contemporary cyber threat and attack settings, and how to defend against them, can be best described from the perspective of the "kill chain" model created by cybersecurity analysts at Lockheed Martin (Hutchins, Cloppert & Amin, 2011). The "kill Chain" model offers a very effective method for understanding contemporary cyber attacks, by outlining each of the seven (7) steps of a typical cyber attack scenario; the model is comprised of the following steps:

- Reconnaissance - studying public information about the target, the target's environment, software mix, practices and software load out.
- Weaponization - preparing a backdoor and a penetration plan intended to deliver a successful attack.
- Delivery - launching the attack and injecting the backdoor.
- Exploitation - triggering the backdoor.
- Installation - installing the backdoor as a bootstrap and any added remote access tools.
- Command and Control - use of the tools to establish remote access
- Actions on Objectives - collection and exfiltration of information, or other actions.

The global nature of the Internet and connectivity of information and communication networks means that cyber attackers can initiate an intrusion from anywhere in the world. Moreover, certain technological advantages enable cyber attackers to be very successful, factors such as low cost, anonymity, speed, diversity of potential sources of attack, the inherent openness of information technology systems, and general lack of knowledge of security awareness of the part of end users. The combination of improved technical capabilities and adaptive tactics have enhanced the ability of nation-states, non state actors, and other nefarious cyber attackers to execute malicious activities, breach defensive perimeters and cause catastrophic damage with impunity. Traditional perimeter defenses and reactive response strategies are no longer adequate. Complex malware that easily evades detection is being developed and deployed at an unprecedented rate. To effectively counter this growing cyber threat, all entities employing information technology must adopt and implement effective cyber intelligence and proactive defense capabilities.

Given the sheer volume and variance in sources of cyber attacks, no one size fit all approach will be sufficient to address the problem. Because each entity, organization structure and network system has unique needs, the functionality of the architecture, system design, and procedures must be considered in crafting a

cyber threat intelligence approach. Counter measures should include comprehensive and proactive operational principles focused on addressing the proliferation of diverse and devastating cyberattacks now targeting American government agencies, critical infrastructure, national and homeland security assets, and commercial enterprises.

According to a 2012 report from the Ponemon Institute, in 2011 the data breaches on the US financial businesses cost between $6.75 million and $31 million dollars. The report noted that in 2008, identity theft cost consumers over $5 billion dollars and other common cyber attacks (fraud and espionage) on businesses and institutions cost over $48 billion dollars. Clearly these types of cyber attacks can be financially devastating. However, their report also showed that taking some protective and preventative cybersecurity actions can have a positive effect, such as reducing the average per capita cost of a data breach from $214 to $194. They suggested that organizations are taking the protection of sensitive and confidential data more seriously in order to avoid costly fines and loss of reputation and brand. (Ponemon Institute, 2012).

The National Research Council (NRC) speculated that a cyber attack on the U.S. power system could knock out power to large regions of the nation for several months (National Research Council, 2012). The Pentagon reported (Nakashima, 2013) that Chinese hackers had stolen designs for more than two dozen major weapons systems deemed critical to U.S. missile defenses and combat aircraft and ships. The rising cyber threat is further evidenced by a series of high-profile cyber attacks targeting U.S. corporations, such as Target, Home Depot and other major retailers. Additionally, a number of similar hacking attacks on major banks websites belonging to Bank of America, JPMorgan Chase and Citigroup, were very effective cyber intrusions that are becoming increasingly common occurrences (Finkle & Rothacker, 2012). These and other recent cyber attacks illustrate the escalating threat that cyber security breaches present to business, government, and individuals relying on these entities for security, safety, health and personal wellbeing.

UNITED STATES ASSESSMENT OF THE CYBER THREAT

Cybersecurity and cyber threats are a relatively new phenomenon and its beginning as a nefarious event can be traced back to a series of high-profile computer crimes in the 1970s and 1980s (Chapple & Seidl, 2015). The earliest documented hacking case and investigation occurred in 1986 when a system administrator at Lawrence Berkley National Laboratory determined that an unauthorized outside party had gained access to the laboratory's computer system. The hacker had obtained sensitive military information on military-related targets, including Army and Air Force installations (Chapple & Seidl, 2015, p 104). The FBI and West German authorities traced the hack back to a German named Markus Hess. Hess was recruited by the Soviet Union's KGB to obtain sensitive U.S. military information; he was arrested and convicted of espionage.

From the Hess attack to the present, the evolution of cyber threats has been marked by a progression from single hacking events perpetrated by lone rangers and script kiddies to more advanced cyber attacks executed by sophisticated marauders, such as nation-states (China, N. Korea, and Iran), nonstate actors (cyber criminals, terrorists, and mercenaries), and loosely organized activist hackers groups (Anonymous and Syrian Electronic Army). In 2009, McAfee, estimated that cybercrime was costing the U.S. $1 trillion a year, a figure used by both President Barack Obama and Gen. Keith Alexander, Commanding General of the military's U.S. Cyber Command, in calls for greater government control of the Internet (Maass & Rajagopalan, 2012). In July 2013, McAfee, in a joint study with the nonprofit Center for Strategic and International Studies, revised its earlier $1 trillion estimate down to $100 billion – one-tenth of the 2009 figure (Gorman, 2013). This could indicate that the federal government lacks a true and reliable assessment tool to accurately quantify the impact of cyber threats, attacks, and events in America. This could be explained by the fact that the private sector owns or controls 80-to-85 percent of the assets potentially affected or targeted by cyber attackers.

In 2008, the Department of Homeland Security reported 5499 known cyber intrusions of U.S. government computer systems, an increase of 40 percent over 2007 totals (Department of Justice, 2011). In 2011, federal, state, and local

government agencies were the target of 11 percent of U.S. data breaches, those breaches combined represented 44 percent of all private and confidential records exposed that year (CSID Inc., 2011). The Defense Department, along with power companies and other major private-sector companies involved in critical infrastructure support, say their firewalls, malware protection tools, and other network safeguards are routinely being tested for vulnerabilities by hackers they believe are working for or with foreign governments such as China and Iran.

Several key U.S. leaders, policy makers, and key officials from law enforcement, the intelligence community, and the military establishment have described the special challenge that cyber threats pose to our economic prosperity, national defense and homeland security. Early in his first term of office, President Obama identified cybersecurity as one of the most serious economic and national security issues facing the nation. Because the President thought the issue was so important, he immediately ordered a thorough review of America's policies and programs focused on securing the country's cyber infrastructure (White House, 2009). In May 2009, the President accepted the Cyberspace Policy Review, which recommended the continuation of the Comprehensive National Cybersecurity Initiative (CNCI) launched by former President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23). President Obama decided that the CNCI would serve as the foundation of a more comprehensive national cybersecurity strategy (White House, 2009).

In October 2012, President Obama continued to demonstrate his concern regarding cyber threats when he signed a highly classified Presidential Policy Directive 20 (PPD-20). The directive, issued as a top secret document, provided a framework for U.S. cybersecurity by establishing principles and processes for offensive and defensive actions in the emerging concepts of cyber war and cyberterrorism. The directive integrated cyber tools with those of national security, and complements Homeland Security Presidential Directive HSPD-23/ NSPD-54. It should be noted that the directive was classified as "Top Secret" and was made public only after it was revealed by Edward Snowden and posted by The Guardian

(Greenwald & MacAskill, 2013), and reported in the Washington Post (Nakashima, 2012). The Washington Post article stated that PPD-20, "is the most extensive White House effort to date to wrestle with what constitutes an 'offensive' and a 'defensive' action in the rapidly evolving world of cyber war and cyberterrorism."

In 2012, General Keith B. Alexander, then head of the National Security Agency and the United States Cyber Command noted that there had been a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011 (Sanger & Schmitt, 2012). This was an acknowledgement by the top American military official responsible for defending the United States against cyber attacks that America's critical infrastructure is coming under attack. Those attacks are considered potentially far more serious than computer espionage or financial crimes. According to testimony from James R. Clapper, Director of National Intelligence, cyber threats have replaced terrorism as the number one global threat to American national security (Clapper, 2013).

UNITED STATES RESPONSES TO CYBER THREATS AND ATTACKS

Both the White House and Congress have initiated action on cybersecurity; however only the President has implemented effective policy that significantly improve the national security posture of U.S. in the cyber realm. In 2008, the President's Comprehensive National Cybersecurity Initiative (CNCI) created the foundation for a whole-of-government approach to protecting the nation from cybersecurity threats. As part of the CNCI, the National Cyber Investigative Joint Task Force (NCIJTF) was established under presidential directive as America's national cybersecurity center (Chabinsky, 2009).

Located in Washington, D.C., the FBI-led NCIJTF serves as the national focal point for coordinating cyber threat investigations. In its role as a headquarters-level task force, the NCIJTF enhances collaboration and integrates operations across the U.S. Intelligence and federal law enforcement communities. The NCIJTF combats cyber crime through a nationwide network of interagency Cyber Task Forces (CTFs) in all 56 field offices focused exclusively on cybersecurity threats. The NCIJTF is also tasked with identifying cyber hackers and understanding their

motivations and capabilities. That knowledge is used to disrupt criminal operations, minimize the consequences of intrusions, and ultimately bring perpetrators to justice. The NCIJTF employs a unified, government-wide approach that leverages intelligence gathering and information sharing among task force partners to gain a strategic view of what cyber actors are trying to do and why (Anderson, 2014).

On February 12, 2013, the President signed an Executive Order - Improving Critical Infrastructure Cybersecurity- focused on enhancing the security and resilience of the Nation's critical infrastructure and maintaining a secure cyber environment; improving coordination and information sharing, and development of the "Cybersecurity Framework" to reduce cyber risks to critical infrastructure. The Cybersecurity Framework requires establishment of a set of standards, methodologies, procedures, and processes to align policy, business, and technological approaches cyber risks (White House, 2013).

On February 25, 2015, the President directed the Director of National Intelligence (DNI) to establish the Cyber Threat Intelligence Integration Center (CTIIC). The CTIIC will be a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers. The CTIIC will also assist relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats (White House, 2015). Clearly, the President and the federal agencies supervised by the Executive Department have an understanding of the growing need to safeguard American information technology and computer systems.

While the White House has demonstrated a degree of urgency and diligence in developing and implementing a comprehensive cybersecurity strategy, the Legislative Branch has failed to craft any laws or regulations for **effectively dealing with cybersecurity (Westby, 2012)**. In 2012, two major bills related to cyber security were reintroduced in Congress. The first, the Cyber Intelligence Sharing and Protection Act (CISPA), passed the House of Representatives in April but failed in the Senate. The second, the Cybersecurity Act, a Senate bill cosponsored by Sens. Joe Lieberman (D-CT) and Susan Collins (R-ME), is pending. As the federal

leadership in the Executive and Legislative Branches of government continue to wrestle with the complex issue of crafting a comprehensive cybersecurity policy, the urgency and necessity for action is being dictated by the pervasive nature of contemporary cyber threats and the frequency of high cost cyber attacks. From a national or strategic perspective, sound cybersecurity policy and effective counter strategies begins with establishing a rigorous regulatory regime and developing a thorough understanding of the cyber threat environment so that any regulation or laws are effective measures for improving cybersecurity.

Today, there are few federal cybersecurity regulations and laws, and the ones in existence focus on specific industries or are very broad in language, intent and purpose. This broad approach lacks rigor, specificity and clarity which create weakness and the vague language of these regulations leaves much room for interpretation as to the regulatory requirements for compliance with the established rules related to cyber security.

Some policy makers believe that the most important cybersecurity problem is the lack of public/private sector collaboration which can be solved through better information sharing between the two sectors. Furthermore, the policy makers believe that the U.S. intelligence community has the necessary expertise to lead the way in this collaboration effort. The Cyber Intelligence Sharing and Protection Act18 (CISPA), an information sharing legislation passed by the House in April 2012, is based on this premise.

Others believe that the most important cybersecurity issue is ensuring that the private sector adequately adheres to standards for critical infrastructure protection and propose that the Department of Homeland Security take the lead in creating a regulatory model. Both the Senate's Cybersecurity Act of 2012 and its Revised Cybersecurity Act of 2012 were based on this premise. The Obama administration is backing the Lieberman-Collins Cybersecurity Act which, in addition to information-sharing, mandates protocols and procedures that the private sector must use to counter cyber threats. In his 2013 State of the Union Address, President Obama announced he had signed an executive order calling for an information-sharing "framework".

CYBER THREAT INTELLIGENCE AND PREDICTIVE ANALYTICS

Thus far, this paper has presented a body of information describing in detail the conundrum facing America, as the country attempts to craft an effective cybersecurity strategy. No matter how daunting the task is it absolutely critical that national cybersecurity measures be created to prevent large scale cyberattacks on key American national security, critical infrastructure, economic and businesses assets. The paper proposes that the contemporary operating environment of cyberspace and the underlying cyber threats requires a comprehensive, relevant, responsive, and actionable strategy to effectively address, deter, and mitigate cyber attacks. The combination of cyber threat intelligence and predictive analytics are the recommended approaches to serve as an overarching intelligence framework for cybersecurity. Together, these two measures can be employed to address many of the cyber threats causing the most damage and harm to information technology and communication networks. The broad purpose of the combined intelligence/predictive analytic approach must be focused on providing actionable intelligence and informing how the user prepares for, prevents, detects, assesses, responds to, manages and recovers from current and emerging cyber attacks.

The exponential expansion of cyber threats and the growing recognition that traditional cybersecurity defensive schemes are failing to adequately protect key network systems have combined to create the urgent need for an innovative and comprehensive cybersecurity strategy to protect information communication technology and critical infrastructure assets.

The term cyber threat intelligence surfaced in technological lexicon in 2009 around the same time as the terms “big data” and “data mining” were becoming common terminology in the cyber domain. Definitions of cyber threat intelligence abounded, and most were patterned after military, intelligence and law enforcement concepts of intelligence analysis.

In a 2013 Gartner report on threat intelligence, cyber threat intelligence was defined as “Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard

to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." (McMillan, 2013).

To achieve a level of contextual relevancy of the threat environment the user organization must implement a thorough intelligence collection and analysis process that involves the identification and monitoring of threat actors and the development of global perspective of the cyber threat environment. The global perspective involve the development of a balanced assessment of the most likely internal and external cyber threats based on capabilities, actions, and intent. The global perspective and strategic relevancy can be enabled through the use of predictive analytic techniques. At the operational intelligence level, understanding the attacker's intentions, targets, capabilities and overall tradecraft will lead to the building of better cybersecurity defenses and the increased capability to defeat advanced persistent threats. Success will be achieved by putting in place the proactive and layered defenses needed to detect and disrupt the steps of the cyber kill chain (Sager, 2014).

By fusing cyber threat intelligence with timely and accurate predictive analytics, the user acquires need–based, accurate and actionable intelligence that can inform their planning, improve their decision making, and help expedite the responses to existing or emerging cyber threats. Predictive analytics encompasses a variety of statistical techniques from modeling, machine learning, and data mining that analyze current and historical facts to make predictions about future, or otherwise unknown, events (Nyce, 2007). It is becoming absolutely critical for organizations to have a cyber threat intelligence capability and a key component of success for any such capability is the ability to not only recognizes the dots but also to connect the dots. While cyber threat intelligence and predictive analytics can help focus and prioritize the list of possible cyber threats they are not expected to address every conceivable type of cyber threat.

CONCLUSION AND RECOMMENDATIONS

Cybersecurity is a complex problem with many different facets, and a portfolio of diverse cyber actors with multiple motives, methods, capabilities and objectives

for perpetrating illicit operations in Cyberspace. Therefore, cyber threat intelligence and related approaches to cybersecurity issues must distinguish not only among different cyber threat actors, such as nation-states, terrorists, criminals, and malicious hackers, but also among different types of cyber threats. For many cybersecurity experts, 2013 was noted as the year of the mega breach. Symantec reported 8 mega breaches with more than 10 million identities exposed per breach representing a 700% increase from 2012 (Symantec Corporation, 2014).

Threats to the nation's cyber assets are real and are being recognized by the Obama Administration and Congress as serious threats to the nation's security, economic prosperity, and critical infrastructure. However, none of the federal government's proposed responses – CISPA, the Cybersecurity Act, or the series of standalone White House executive orders – will be effective by themselves. They are either too vague, duplicate or overlap existing laws, and seem to grant sweeping powers to the government to gather and process cyber information without discrete limits or proper oversight. Traditional approaches for cyber security, that focus primarily on static methods, such as firewalls perimeter defenses, and end point security are necessary but insufficient.

Therefore, this paper recommends that all organizations in the public and private sectors and operating in the cyberspace environment implement a cyber threat intelligence approach complemented with some form of predictive analytic techniques. The combination should be crafted and implemented as key component of a defense-in-depth strategy involving a proactive defensible scheme. The defense-in-depth concept is based on building multiple layers of protection between the attackers and the protected systems, data, and networks (Chapple & Seidl, 2015). For example, the U.S. Computer Emergency Readiness Team recommends a defense-in-depth structure consisting of multiple strong layers: security policies and procedures; updated firmware; patched operating system; vulnerability awareness (intrusion detection systems and security information and event management); effective firewall techniques; and trained staff with the appropriate level of expertise.

The effective implementation of cyber threat intelligence is about reducing vulnerabilities and risk in cybersecurity, and the complementary use of predictive

analytic techniques is about obtaining relevant information to enhance the intelligence process. The combined use of the two concepts is focused on the goal of establishing actionable intelligence for effective problem solving, improved decision making, and enhancing cybersecurity measures.

REFERENCES

[1] Anderson, Jr., R. (2014). The cyber threat and FBI response. Statement before the Senate Committee on Homeland Security and Governmental Affairs Washington, D.C. Retrieved from http://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security.

[2] Bailey, B. (2015). Anthem hackers tried to breach system as early as Dec 10. Associated Press. Retrieved from http://www.huffingtonpost.com/2015/02/06/anthem-hackers-december_n_6634440.html.

[3] Chabinsky, S.R. (2009). The cyber threat and the FBI's cyber program. Statement before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security. Washington, D.C. November 17, 2009. Retrieved from http://www.fbi.gov/news/testimony/collections/2009-testimonies.

[4] Chapple, M. & Seidl, D. (2015). Cyberwarfare: Information operations in a connected world. Burlington, MA: Jones and Barnett Learning.

[5] Cheney, J.S. (2010). Heartland payment systems: Lessons learned from a data breach. Retrieved from http://www.phil.frb.org / consumer-credit-and-payments / payment-cards-center / publications / discussion-papers / 2010 / d-2010-january-heartland....

[6] Clapper, J.R. (2013). Worldwide threat assessment of the US intelligence community: Hearing before the Senate Select committee on intelligence, 113th Congress.

[7] CSID Inc. (2011) Resources: Data breaches by industry. Retrieved from http://www.csid.com/resources/stats/databreaches- by-industry/, citing data from 2011 Breach Statistics Report, Identity Theft Resource Center.

[8] Department of Justice. (2011). The Federal Bureau of Investigation's ability to address the national security cyber intrusion threat. Office of the Inspector General Audit Division. Audit Report 11-22. Retrieved from http://www.justice.gov/oig/reports/FBI/a1122r.pdf.

[9] Farnham, G. (2013). Tools and standards for cyber threat intelligence projects. SANS Institute White Paper. Retrieved from http://www.sans.org / reading-room / whitepapers / warfare / tools-standards-cyber....

[10] Finkle, J., & Rothacker, R. (2012). Exclusive: Iranian hackers target Bank of America, JPMorgan, and Citibank. Reuters. Retrieved from http://www.reuters.com / article / 2012 / 09 / 21 / us-iran-cyberattacks-idU...

[11] Gorman, S. (2013). Annual U.S. cybercrime costs estimated at $100 Billion. *The Wall Street Journal*, July 22, 2013. Retrieved from http://online.wsj.com/article/ SB10001424127887324328904578621880966242990.html.

[12] Greenwald, G. & MacAskill, E. (2013). Obama orders US to draw up overseas target list for cyber-attacks *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

[13] Hutchins, E., Cloppert, M. and Amin, R. (2011). Intelligence-driven computer network defense. Proceedings of the 6th International Conference on Information Warfare, 2011. Retrieved from http://www.isightpartners.com/2014/09/strenghtening-cyber-kill-chain-cyber-threat-intelligence-part-1-of-2/#sthash.bbxIn9IQ.dpuf.

[14] Marci, G. (2015). Clapper: Sony hack 'most serious' cyber attack on U.S. so far. The Daily Caller. Retrieved from http://dailycaller.com / 2015 / 01 / 07 / clapper-sony-hack-most-s /.

[15] Maass, P. and Rajagopalan, M. (2012). Does cybercrime really cost $1 trillion? ProPublica Online. Retrieved from http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

[16] McMillan, R. (2013). Definition: Threat intelligence.

[17] Mezzour, G., Carley, L.R., and Carley. K. M. (2014a). Longitudinal analysis of a large corpus of cyber threat descriptions. Journal of Computer Virology and Hacking Techniques. DOI 10.1007/s11416-014-0217-8

[18] Mezzour, G., L., Carley, L.R., and Carley, K. M. (2014b). Global mapping of cyber attacks. Carnegie Mellon University, School of Computer Science, Institute for Software Research, Technical Report CMU-ISR-14-111.

[19] Nakashima, E. (2012). Obama signs secret directive to help thwart cyberattacks. *The Washington Post*. Retrieved from http://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense.

[20] Nakashima, E. (2013). Confidential report lists U.S. weapons system designs compromised by Chinese cyber spies. *The Washington Post*. Retrieved from http://articles.washingtonpost.com/2013-05-27/ world/39554997_1_u-s-missile-defenses-weapons-combat-aircraft.

[21] National Defense Strategy of the United States of America (2005). Retrieved from http://www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm.

[22] National Research Council. (2012) Terrorism and the electric power delivery system. Washington, DC. National Academies Press,

[23] Nyce, C. (2007), Predictive analytics white paper. American Institute for Chartered Property Casualty Underwriters/Insurance Institute of America. Retrieved from http://www.tcs.com / Site Collection Documents / White Papers / Consulting_Whitepaper... .

[24] Oracle (2010). Predictive analytics: Bringing the tools to the data. Oracle White Paper.

[25] Pellerin, C. (2015). Cyber threats blur roles, relationships. Department of Defense News, Defense Media Activity. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=128305.

[26] Ponemon Institute (2012). 2011 Cost of data breach study: United States. Retrieved from http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf.

[27] Rosenzweig, P. (2012). The alarming trend of cybersecurity breaches and failures in the U.S. government. The Heritage Foundation. Backgrounder No # 2695. Retrieved from http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government.

[28] Sager, T. (2014). Killing advanced threats in their tracks: An intelligent approach to attack prevention. A SANS Whitepaper. Retrieved from http://www.sans.org / reading-room / whitepapers / analyst / killing-advanced-threats....

[29] Sanger, D.E. and Schmitt, E. (2012). Rise is seen in cyberattacks targeting U.S. infrastructure. New York Times. Retrieved from www.nytimes.com/…12/07/27/us/cyberattacks-are-up....

[30] Siegel, Eric (2013). Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die (1st Ed.). Hoboken, NJ: John Wiley & Sons.

[31] Strohm, C. (2015). FBI provides more proof of North Korea link to Sony hack. Bloomberg Business Online. Retrieved from http://www.bloomberg.com / news / articles / 2015-01-07 / clapper-warns-of-more-po...

[32] Symantec Corporation. (2014). Internet Security Threat Report 2014. Symantec Corporation. Retrieved from http://www.symantec.com / connect / blogs / symantec-2014-internet-s... .

[33] Trend Micro Incorporated. (2013). *Trend Micro Security News*. "Blurring boundaries: Trend micro security predictions for 2014 and beyond. Retrieved from http://about-threats.trendmicro.com/us/security-predictions/2014/blurring-boundaries/.

[34] Westby, J. (2012). Congress needs to go back to school on cyber legislation. Forbes Online. Retrieved from http://www.forbes.com/sites/jodywestby/2012/08/13/congress/.

[35] White House. (2009). Remarks by the president on securing our nation's cyber infrastructure. Office of the Press Secretary. Retrieved from www.whitehouse.gov/…press_office/Remarks-by-the... ... 2009 .

[36] White House. (2013). Executive order: Improving critical infrastructure cybersecurity. Office of the Press Secretary, February 12, 2013. Retrieved from www.whitehouse.gov/…_press_office..

[37] White House. (2015). Fact sheet: Cyber threat intelligence integration center. Office of the Press Secretary, February 25, 2015. Retrieved from https://www.whitehouse.gov / the-press-office / 2015 / 02 / 25 / fact-sheet-cyber-threat-....