International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(1): 31-37
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-0012

Implication of Cyber Warfare on the Financial Sector. An Exploratory Study

[1]Sohail Razi Khan,
[1] Higher Colleges of Technology, Computer Science Department, Sharjah, UAE
Skhan1@hct.ac.ae

ABSTRACT

The cyber domain is constantly evolving, providing both new opportunities and challenges for financial services institutions. The implication of cyber warfare on the financial sector is serious where state and non-state actors are involved to settle geo-political tensions. To improve cybersecurity, financial services institutions, like many other organizations, must elevate the topic and address threats holistically to the highest levels of the organization in a manner that they understand. In this effort, the need is to understand threats. Just as the likelihood and impact of cybercrimes varies, so should the responses to them. This paper examines the implication on the financial institution due to cyber warfare. It provides how state non-state actors are involved to attack the financial institutions across the world. The paper provides an exploratory study by involving the financial institutions to investigate the challenges of cyber warfare and its implications on the financial sector.

Key Words

Cyber Warfare, DDoS (Distributed Denial of Service) attack, APT (Advanced Persistent Threat), State-sponsored attacks, Financial regulations

I. INTRODUCTION

As we speak, cyberattacks are threatening the financial institutions across the world. Different level of sophistication has been carried out ranging from a low-level amateur attack to a coordinated sophisticated intrusion. From a long time, the financial institutions are under direct assault from a range of cyber criminals causing loss of billions of dollars. This has casted doubt on the capability of the financial sector most of which is operating in the private sector to secure personal data over their systems [1]. The cyberattacks are focused on conflicting unrepairable damages on financial institutions as they have global presence and financial gains can be made [2]. There are many examples that were reported of successful cyberattacks on various banks which had serious financial implication for banks and their customers. One of the major breach that was reported in January, 2014 by JP Morgan Chase & Co., which is the largest American bank by assets announced, that more than 76 million customer records with seven million business customer records were compromised [3]. The attack which was originated from Russia was so complex in nature that it went unnoticed for months even though bank was spending nearly $250 million in the cybersecurity enhancement program. The hackers were successful to steal personal information related to customers and considered to be responsible of at least one dozen other hacking attempts on various financial institution. The security experts have shared their concerns that attackers who were involved in the attack would have left backdoors into JPMorgan's network and there is possibility of undetected intrusion still exist. This financial security breach is considered as one of the largest breach that sends a clear message to all the financial sectors that their network is not safe and can be exploited.

The Treasury Department, Secret Services, Federal Bureau of Investigation (FBI), and U.S. intelligence agencies have worked with JPMorgan after the intrusion and after detailed forensic investigation shared their findings that this new stealth attack can be initiated from a state actor. The findings from the report indicate that the attack can be in response to Western sanction on Russia. The findings from the National Security Agency, that Russia has used proxies to attack JPMorgan's network [4]. The attacks on financial sectors and especially in the case of JPMorgan is identifying the new face of cybercrime to exploit the cyber weakness in the infrastructure to gain profit but at the same time presents a new asymmetric state warfare that can be deployed by less powerful states to conflict damage on powerful states across the world [5]. The cyber warfare was used as asymmetric strategy by North

Korea to hack Sony systems in December, 2014 that included the destruction of data, publication of sensitive internal communication and threat of violence in retaliation of U.S. sanctions and release of the movie 'The Interview'. The frequency and type of sophistication used to attack the financial sector is increasing and recently CitiBank reported ten million cyberattacks on its system every month which is an alarming situation [6]. This scenario is changing where financial institution is facing the convergence between economic and cyber warfare where financial sector has to fight battles not only in the boardroom but have to ready for geopolitics front where cyber tools will be used as a commercial weapon [7].

The paper is organized as follows. First of all, Section II contains the evolution of cyber financial threat model followed by Section III explains the Cyber threats to financial sectors. Section IV explains the Cyber tools and techniques used to carry out of cyber-attack. The next section of the paper contains Exploratory Study: Cyber-attacks on the Banking Sector followed by conclusion.

II. EVOLUTION OF CYBER FINANCIAL THREAT MODEL

The financial sector across the world is a driver of globalization and commercial order but internal system vulnerabilities can lead to disorder. Most of the developed economies are dependent on the financial sectors to provide growth and prosperity to masses. The weakness of these developed economies is not in-terms of physical resources or knowhow of technical knowledge but more reliance on these virtual systems. As reinforced by former Director of National Intelligence Mike McConnell, as we are more dependent on the virtual systems, in case we face cyberwar we will lose [8]. The Internet contributed an estimated 18% to the U.S. GDP between 2010 and 2015 and 35% of total Internet revenues earned by the top 250 Internet-related companies in the world. The cyber warfare provides a new frontier on the geopolitical competition. The cyber criminals are attacking the financial sector by stealing billions of dollars' worth intellectual property every year. According to the latest figures cost of cybercrime to the global economy is more than $500 billion annually [9]. Various attacks have taken place against the International Monetary Fund (IMF), Lockheed Martin's information system (via stolen SecureID data), Citibank, Google's mainframes, Bank of America and Sony's PlayStation data.

Cyber warfare is used to steal national secrets of an enemy state and use it for their own financial and political advantage. The cyber financial threat model is evolving in order to dominate the world order, inflict massive financial damage to the opponent and use it have a strategic advantage. In August 2011, McAfee Internet security firm reported one the largest attack in which more than 72 business organizations and companies around the world have their system breached by unidentified hacker from China. The report identifies that the main goal of the attack was to steal business secret, new product research and development designs to design and produce better competing products. This attack according the report has resulted in major financial loss for these companies. The report also identified details of several U.S oil companies between 2008-2010 sensitive research and development files were compromised due to these attacks. The research files contained important bidding details prepared by U.S oil companies for oil-field research across the world. Due to this breach, there was massive financial loss for these oil companies and provided unfair advantage to their competitors [10]. According to the report published by technology firm FireEye, China has threatened Australia key sectors including data theft from mining and natural resources firms [11]. The report identifies major financial loss for these sector which faced four 'zero-day' vulnerabilities in Microsoft's Windows operating system while maintaining a low profile points directly to a state-sponsored entity.

The cyber financial threat model is evolving as some countries are using cyber warfare as strategy to exercise power, gain political advantage and inflict financial losses over their

competitors. Cyberspace has created opportunities for state and non-state actors to inflict financial damages, settle political scores and create confusion among adversaries. There is clear evidence that state-sponsored cyber warfare is intensifying as a part of increasing cyber arm race. The evidence of state actor using cyber warfare is becoming a norm where the most prominent attack was carried out in the form of 'Stuxnet' virus designed by U.S. and Israel to sabotage Iranian nuclear facilities and discovery of 'Gauss' virus by Moscow-based security firm Kaspersky Lab, that infected nearly 2500 computers in Israel and Palestinian tied to Lebanese bank. The focus of virus was to capture transaction data from Lebanese banks and capture financial data. The Lebanese bank are considered as secretive in the world and the purpose behind the attack was to find the money transferred to various countries such as Iran, Syria, Hezbollah [12]. The Iranian response was even more devastating in-order to respond to the financial assault on its economy and currency. The hackers named as Izz ad-Din Al-Qassam Cyber Fighters conducted a large scale of denial-of-service attack against the banking systems of JPMorgan Chase, Citigroup, PNC Bank, Wells Fargo, U.S. Bancorp and Bank of America. The attackers increased fake demands on the banks sites that was increased more than 20 times leading to suspending the entire banking operations. In December 2012, a new hacker group calling themselves "Cutting Sword of Justice" attacked the Saudi Arabia's national oil company Aramco computer systems destroyed data from 30,000 computers and created disruption for the entire operations.

According to the World Economic Forum's Global Risk 2015 report, cyber financial threat model keeps evolving where cyberspace will be at the focal point of both geopolitical and economic world, which will be a serious challenge. Using cyber warfare to conflict financial damages where geopolitical equation is the new variable and difficult to predict the development of such situation [13]. The cyberattack continues to threaten the financial system with increasing frequency which is resulting in disruption of the financial order and geopolitical relationship continues to be factor for these cyber-attacks. All these viruses show a pattern of evolution in the cyber threat model where the state or non-state actors are willing to use cyber weapons to impact financial and other sectors to achieve their strategic goals. This evolution of the cyber threat model raises serious questions in the overall stability of the global financial systems. The questions is raised, how the financial system continues with its operations when faced with indecipherable payload that can damage the entire infrastructure?

III. TYPE OF CYBER THREATS TO FINANCIAL SECTOR

According to the cybersecurity experts there are different types of threats to the financial sector. The most sophisticated cyber actor is designed by the state to use espionage to steal intellectual property, hack financial data from the banks and interrupt their entire operations. The second type of attacker target the bank as they are considered as a symbol of any country and due to geopolitical tensions, those symbols are considered as a fair target. Third type of attacks that are carried against the financial system are "hacktivist" who take advantage of the vulnerabilities in the infrastructure of IT system. The main goal is to achieve publicity and promote political influence. The next type of attacker are organized criminal who use cyber warfare to steal money from the financial institutions without being detected [14]. There is financial gain to be made from these cyber-attacks. The state and non-state actors are increasingly training their sights on banks and desire to exploit their vulnerabilities.

The recent report from the Office of the Comptroller of Currency's Semi-Annual Risk [15], showing a very alarming trend of increased cyberattacks on the financial institutions. According to the report criminal attacking financial institutions are becoming better at accessing bank information as the intrusion technologies are becoming better and tools are

easily available to conduct attacks. The report further states, there are abundant of hackers available over internet to be hired to carry out attacks. In July 2014, Bloomberg's Businessweek magazine reported that Russian hackers had stolen the Nasdaq records in 2010 [16]. State-sponsored attacks are not only limited to a region or type. The Advanced Persistent Threat 1 (APT1), was described by Mandiant in 2013 report as "one of the most prolific cyber-espionage groups in terms of the sheer quantity of information stolen" and stated the group had stolen terabytes of data from at least 141 organizations in 20 major industries. In March 2013, the "Dark Seoul" attacks targeted South Korean banks and financial institutions in the country. Due to the attack the hackers were able to deleted data from hard drives, targeted ATMs and mobile payment platforms, overloaded bank servers and shut down computers at several South Korean banking systems.

IV. CYBER TOOLS AND TECHNIQUES TO ATTACK

There are range of cyber tools, techniques and actors to attack the financial and banking sector. With the passage of time the international actors engaged in cyberattacks has complicated the threat model. The ease by which intrusion tools are available in the public domain has increased the number of attacks. The cyber criminals or agents of the hostile power can mount attack on the vital part of an economy such as power station, electrical grid and communication networks. Financial Trojans represent the newest type of attack and a major threat to the banking sector. According to the report published from Symantec in 2015, the financial Trojans targeted over 1,400 financial institutions and the top 15 most targeted financial institution were targeted by over 50% of known Trojans. The number of Trojan attacks has quadrupled and requires a detailed countermeasure to stop the attack.

The next major type of attack is the DDos (Distributed Denial of Service) attacks on the financial system. In 2016, over 720 million identities were exposed and the attacks went up more than 32% from 2014 with 28 zero-day vulnerabilities that were discovered [15]. Attackers add watering-hole attack to their arsenal in which threat actor compromise a carefully selected website by inserting an exploit resulting in malware infection. The next type of attacks is the death by spear-phishing on the financial sector in which attacker disguise himself as a friend or known entity to ask for sensitive information [16]. Ransomware scams in which attackers pretend to be local law enforcement demanding a fake fine. The next threat to the financial sector can be "Cryptolocker" scam where attacker pretend to be law enforcement and at the same time they will encrypt the user files and request for a ransom for the files that are encrypted [17]. Most of us are using mobile phones to access our banking records. The mobile malware has an explosive growth and according to the report publish by The Norton Report, 2015 a global survey of end-users showed 42% of mobile users had experienced mobile cybercrime [18]. In this environment, it is becoming difficult to differentiate state from non-state actors. Many state actors such as Russia has put up cyber aggression and use this technique to support its political agenda. The financial institutions are under a range of different type of attacks and this is an alarming situation for financial institution.

V. AN EXPLORATORY STUDY: CYBER-ATTACKS ON BANKING SECTOR

Cyberattacks are common on the financial sectors leading to massive losses. According to the 2015 Global Financial Services Industry Security Study from Deloitte, one-quarter of all banks were victim of cyber breach in 2015 [19]. According to the Norton Cybercrime report the global annual cost of cybercrime to consumers is $110 billion [20]. According to the survey from the high street banks, it was evident that low-level spams, malware are a concern and one in two banks have reported phishing events in the past two years while more than one in three have

been infected by both malware and mobile malware. Only 6% of the banks stated that they have not experienced any cyber incidents.

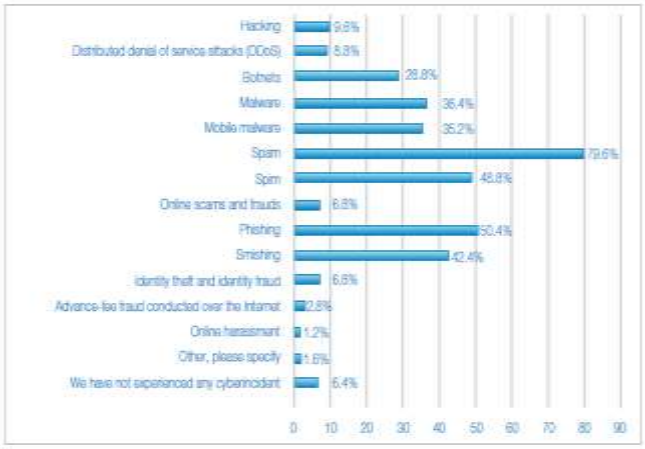

Figure 1: Proportion of banks reported cyber incident in past two year [20]

According to the survey, nearly twice as many of the 250 banking executives polled 78% stated cybersecurity as a 'significant' risk to their organization. More than 82% executives stated that rate of increase of financial losses from cyberattacks is rising at unacceptable level. The survey reveals that their organization have experienced a wide variety of cyber incident over past two years. Spam, spim, malicious software, mobile malware, phishing and botnet are just some of the most common cited incident.

The cyber threat in the banking sector doesn't have equal concern. When combining the likelihood and impact of various crime some threats stand out. As mentioned in the Figure 2, phishing is technique used to get users information is seen as having the highest impact on banks combined with a high likelihood of attack. The survey is worrying as retail banks 59% of retail bank executive reported incident of phishing, compared with 40% of commercial bank executives.

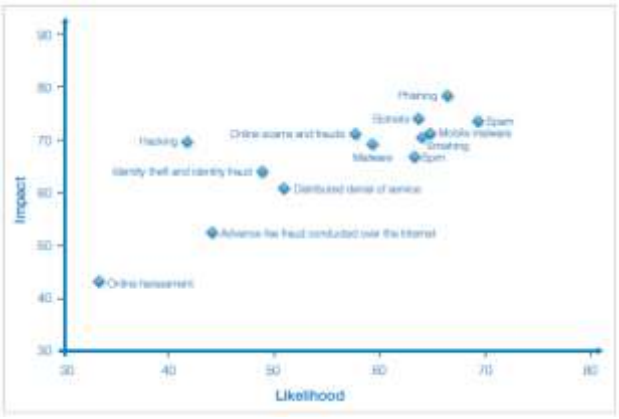

Figure 2: Identification of most likely risk and most severe risks.

DDoS (Distributed Denial of Service) attacks, which is considered as a less concern to the banks. Nearly 72% of respondents stated there is an increase in the political dimension to the threat faced. According to survey there is a new set or worrying threat vector generally described as 'hacktivism'. This attack inflicts the reputational damage to the business. According to the Figure 2, the Spam, has more likelihood and severe impact on the financial sectors.

According to Figure 3, there is ongoing evolution of technologies leads to rapidly changing threat environment. According to the survey, 39% respondents rate technology limitation and 38% difficulties in keeping pace and rapidly changing cyber risks. 34% respondents stated there is a high cost of addressing or mitigating risk in the financial sectors. This is concerning because as the risk radar mentioned in the Figure 2, illustrates threats are seen as having widely differing impact and organization currently appear to be catching up in using the latest technologies to mine their data proactively. The survey clearly indicates there is a learning curve in keeping up with the latest threats as they are constantly evolving and changing.

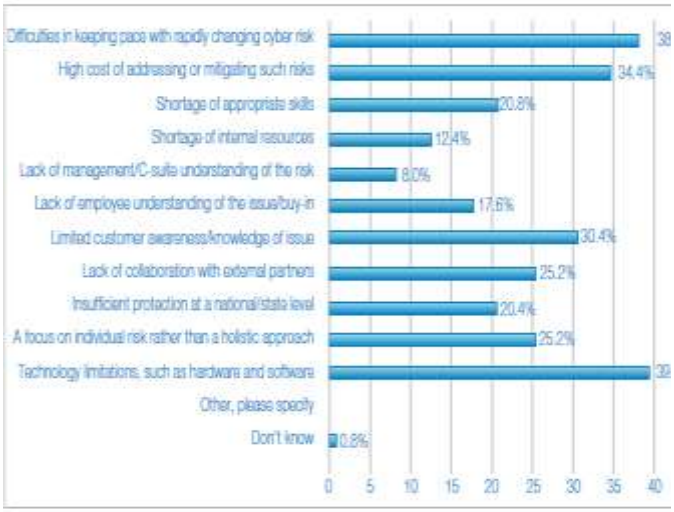

Figure 3: Key Challenges in dealing Cybersecurity Threats

Due to cyberattacks these banks have faced massive financial losses according to the survey results. In the figure 4, more than 23.1% banks have reported significant impact in-terms of financial losses in the bank due to cyber-attacks and 64.1% reported moderate impact in-terms of financial loss due to cyberattacks. As reinforced in the Figure 4, due to cyberattacks more than 39.3% banks considered having significant impact on the trust in our banking services from the existing customers whereas 32.1% consider having moderate impact on the trust in banking services from existing customers.

As stated in the Figure 4, 21.8% banks stated significant impact on the brand and reputation due to these cyberattack and 54.7% think moderate impact on the brand and reputation of the bank due to cyberattacks.

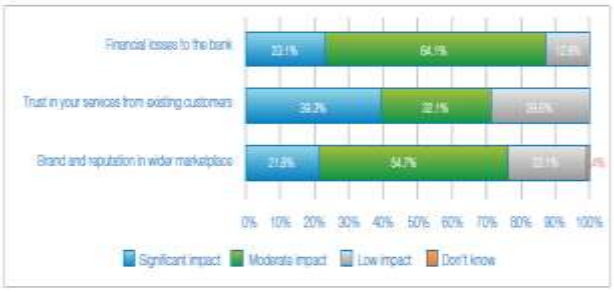

Figure 4: Impact of Cyberattacks Bank's Business

VI CONCLUSION

The cyber domain is constantly evolving, providing both new opportunities and challenges for financial services institutions. To improve cybersecurity, financial services institutions, like many other organizations, must elevate the topic and address threats holistically to the highest levels of the organization in a manner that they understand. In this effort, the need is to understand threats. Just as the likelihood and impact of cybercrimes varies, so should the responses to them. In this effort, banks need to distinguish between financially motivated attacks and those that are non-financial in nature. Cooperate externally with all entities outside the bank. Banks are perceived as operating in silos, but greater external cooperation should enhance their cybersecurity efforts more broadly. Criminals often target weaker links in the banking ecosystem, and it would be in the banks' long-term interests to help third-party actors improve their own cybersecurity efforts. Improve awareness among all stakeholders. Greater communication between the technical and business functions is necessary to improve cybersecurity within enterprises. By educating everyone from end users and employees to top management, banks must continue to improve educational efforts surrounding cybersecurity.

REFERENCS

1. Kara Scannell & Tom Braithwaite, "Fidelity Hack Points to JPMorgan Link," *Financial Times*, October 9, 2014. (http://www.ft.com/intl/cms/s/0/2564f64e-4f2e-11e4-9c88-00144feab7de.html#axzz3GJX0s0Ma)

2. Emily Glazer & Danny Yadron, "J.P. Morgan Says About 76 Million Households Affected By Cyber Breach," *The Wall Street Journal*, October 3, 2014. (http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372)

3. In a *Financial Times* interviews, Frank Abagnale—inspiration for *Catch Me If You Can* and anti-fraud specialist—is dubious that the hackers would not have taken additional data. "The Benefits of Being a Real Fraudster," *Financial Times*, October 9, 2014. (http://www.ft.com/intl/cms/s/2/1e7ad07c-4ae4-11e4-839a-00144feab7de.html#axzz3GJX0s0Ma)

4. "Obama Had Security Fears on JPMorgan Data Breach," *DealBook*, accessed October 16, 2014. (http://dealbook.nytimes. com/2014/10/08/cyberattack-on-jpmorgan-raises-alarms-at-white-house-and-on-wall-street/)

5. Joel Brenner, "Nations Everywhere Are Exploiting the Lack of Cybersecurity," *The Washington Post*, October 24, 2014. (http:// www.washingtonpost.com/opinions/joel-brenner-nations-everywhere-are-exploiting-the-lack-of-cybersecurity/2014/10/24/ 1e6e4b70-5b85-11e4-b812-38518ae74c67_story.html)
6. "Finextra: MasterCard Unveils Tool to Tackle Cyber Threat," *Finextra*, October 2, 2014. (http://ww.finextra.com/news/ fullstory.aspx?newsitemid=26532&topic=sibos)
7. Charles Blauner, Global Head of Information Security for Citi Bank and the Chair of the Financial Services Sector Coordinating Council, "The Cyber Wars Escalate," *SIBOS Conference*, September 30, 2014.
8. Barry Vengerik et al., "Hacking the Street? FIN4 Likely Playing the Market," *FireEye*, 2014. (https://www2.fireeye.com/ fin4.html)
9. Mike Rogers, "Stopping the Next Cyberassault," *The Wall Street Journal*, December 25, 2014. (http://www.wsj.com/articles/ mike-rogers-stopping-the-next-cyberassault-1419543945)
10. Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (PublicAffairs, 2013).
12. Kara Scannell, "NY Bank Regulator Targets Cyber Threat," *Financial Times*, October 6, 2014. (http://www.ft.com/ intl/cms/s/0/5a981338-4cdf-11e4-a0d7-00144feab7de. html#axzz3GJX0s0Ma)
13. Trudy Rubin, "It's Time to Get Serious about Cyber Attack Risk," *Sydney Morning Herald*, December 29, 2010. (http://www. smh.com.au/federal-politics/political-opinion/its-time-to-get-serious-about-cyber-attack-risk-20101228-1998p.html)
14. David E. Sanger & Eric Schmitt, "Cyberattacks Are Up, National Security Chief Says," *The New York Times*, July 26, 2012. (http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html)
15. "Net Losses: Esatimating the Global Cost of Cybercrime," *Center for Strategic and International Studies* June 2014. (http:// csis.org/event/2014-mcafee-report-global-cost-cybercrime)
16. Ellen Nakashima & Ashkan Soltani, "FBI Warns Industry of Chinese Cyber Campaign," *The Washington Post*, October 15, 2014. (http://www.washingtonpost.com/ world/national-security/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b-f6333e2c0453_story.html)
17. Ibid.
18. "Double-Edged Sword: Australia Economic Partnerships Under Attack from China," *FireEye Blog*, October 13, 2014. (http://www.fireeye.com/blog/technical/2014/10/double-edged-sword-australia.html)
19. James Andrew Lewis, "The Key to Keeping Cyberspace Safe? An International Accord," *The Washington Post*, October 7, 2014. (http://www.washingtonpost.com/postlive/key-to-keeping-cyberspace-safe-international-accord/2014/10/07/ae50a35e- 4812-11e4-b72e-d60a9229cc10_story.html)
20. "Hashcat's GPU-Accelerated Gauss Encryption Cracker—," *Securelist*, December 28, 2012. (https://securelist.com/blog/ events/34884/hashcats-gpu-accelerated-gauss-encryption-cracker-4/)
21. Kim Zetter, "Researchers Seek Help Cracking Gauss Mystery Payload," *WIRED*, August 14, 2012. (http://www.wired. com/2012/08/gauss-mystery-payload/)
Expand to Banks and Neutral States?" *The Atlantic*, August 17, 2012. (http://www.theatlantic.com/international/archive/2012/08/did-the-bounds-of-cyber-war-just-expand-to-banks-and-neutral-states/261230/)
23. David Nordell, "Is the New 'Gauss' Malware a Counter-terror Finance Intelligence Tool?" *The Terror Finance Blog*, August 12 2012. (http://www.terrorfinanceblog.com/2012/08/is-the-new-gauss-malware-a-counter-terror-finance-intelligence-tool. html)
24. "Deconstructing the Al-Qassam Cyber Fighters Assault on US Banks," *Recorded Future*, January 2, 2013. (https://www. recordedfuture.com/deconstructing-the-al-qassam-cyber-fighters-assault-on-us-banks)
25. E. Scott Reckard, "Banks Fail to Repel Cyber Threat," *Los Angeles Times*, September 27, 2012. (http://articles.latimes. com/2012/sep/27/business/la-fi-bank-attacks-20120927)
26. Harald Malmgren and Mark Stys, *Computerized Global Trading 24/6: a Roller Coaster Ride Ahead?: An Article from: The International Economy*, n.d.
27. Rob Lati, "The Real Story of Trading Software Espionage," *Wall Street & Technology*, July 10, 2009. (http://www. wallstreetandtech.com/trading-technology/the-real-story-of-trading-software-espio/218401501)
28. U.S. Commodity Futures Trading Commission & U.S. Securities & Exchange Commission, "Findings Regarding the Market Events of May 6, 2010," September 30, 2010, page 13. (http://www.cftc.gov/ucm/groups/public/@otherif/documents/ ifdocs/staff-findings050610.pdf)
29. "2.2 Global Risks Arising from the Accelerated Interplay Between Geopolitics and Economics," *World Economic Forum*, accessed January 30, 2015. (http://reports.weforum.org/global-risks-2015/part-2-risks-in-focus/2-2-global-risks-arising-from-the-accelerated-interplay-between-geopolitics-and-economics/)
30. Martin Arnold, "Banks Face Rising Threat from Cyber Crime," *Financial Times*, October 6, 2014. (http://www. ft.com/intl/cms/s/0/5fd20f60-4d67-11e4-8f75-00144feab7de. html#axzz3FOFcGxgh)
31. "Net Losses: Esatimating the Global Cost of Cybercrime," *Center for Strategic and International Studies* June 2014. (http:// csis.org/event/2014-mcafee-report-global-cost-cybercrime)