International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Hackers Portfolio and its Impact on Society

Dr. Adnan Omar & Terrance Sanchez, M.S.
6400 Press Drive
Southern University at New Orleans

ABSTRACT
Currently, a hacker is defined as a person using computers to explore a network to which he or she did not belong. Hackers find new ways to harass people, defraud corporations, steal information and maybe even destroy valuable information by infiltrating private and non-private organizations. According to recent research, bad hackers make up only a small minority of the hacker community. In today's society, we depend on more technology than ever and that increases the likelihood of hackers having more control over cyberspace. Hackers work by collecting information on the intended target, figuring out the best plan of attack and then exploiting vulnerabilities in the system. Programs such as Trojan horses and Flame viruses are designed and used by hackers to get access to computer networks. This paper describes how hacker behavior is aimed at information security and what measures are being taken to combat them.

Keywords
Types of Hacker, Security, Technology, Cyberspace.

1. INTRODUCTION
Hacking is a very serious problem that can severely compromise your computer. If your computer is connected to the Internet, you are vulnerable to cyber-attacks from viruses and spyware. It is virtually impossible to stop a determined and skilled hacker from breaching most home network security measures commercially available [1]. The primary objective of hacking is to gather information and documents that could compromise the security of governments, corporations or other organizations and agencies. In addition to focusing on diplomatic and governmental agencies around the world, the hackers also attack individuals as well as groups.

The computer term "hacker" can refer to a good or bad reputation according to the mass media. Hackers have developed new ways to use computers since their invention, and create programs that no one else can, to utilize their potential. Hackers are motivated by various reasons which may range from bold ideas, lofty goals, great expectations or simple deviation from the norm as well as the excitement of intrusion into a complicated computer system. In the past, hacking has been used to hassle an intended victim, steal information, or spread viruses. Not all hacking results from premeditated malicious intent. Most hackers are interested in how computer networks function and barriers between them and that knowledge is considered a

challenge to their intelligence. However, some use their knowledge to help corporations and governments construct better security measures. Although we have heard about mischievous hackers sabotaging computers, networks, and spreading viruses, most of the time hackers are just driven by the curiosity they have about how different systems and programs work. Although malicious and intrusive methods may be representative of what hackers do, many of the methods and tools used by them are constructive in fixing glitches in software as well as focusing on the vulnerability of computer technology. It is through exposure of these vulnerabilities that new ideas and better security measures are created.

When someone hears the word "hacker" one might immediately conjure images in the mind's eye of a criminal; more specifically, a criminal sitting at a computer typing away with a screen reading "Access Denied." That image in mind, one has the mainstream image of a modern day hacker. In today's society, hacking is just as prevalent as it has been in years past. Viruses are still coded every day, worms still crawl the internet, and Trojan horses continue to allow back door access into computer systems [2].

Even within hacker society, the definitions range from socially very positive to criminal. In [3], there are two basic principles hackers live by: first, is that information sharing is a powerful good and that it is the ethical duty of hackers to share their expertise by writing free software and facilitating access to information and to computing resources whenever possible. Second, is that system cracking for fun and exploitation is ethically OK as long as the cracker commits no theft, vandalism or breach of confidentiality. It differentiates between benign and malicious hackers based on whether damage is performed, though in reality all hacking involves intrusion and a disregard for the efforts, works and property of others.

This research has reviewed the literature on hackers and it identifies countries, reasoning, and type of penalties that are most likely to be involved in hacking activities. In addition, it will address the steps that are needed to put in place in order to reduce hacking and the type of penalties.

2. LITERATURE REVIEW

Electronic information is a critical part of our culture. Yet no matter where the technology has taken us, the fact remains that what happens in cyberspace has tangible impacts on each of our lives. Therefore, it is as important for us to be secure in cyberspace as it is in our physical world [4]. According to a report from McAfee based on a survey conducted globally on more than 800 IT company CEO's in 2009, data hacking and related cybercrimes have cost multinational companies one trillion U.S. dollars [5].

The media often presents hackers as having a thrilling reputation. Adolescents who are lacking the social skills required to be accepted by others may fantasize about their degree of technological skills, and move online in search of those who profess to have technological skills the student desires. A simple search using the term "hacker" with any search engine, results in hundreds of links to illegal serial numbers, ways to download and pirate commercial software, etc. Showing this information off to others may result in the students being considered a "hacker" by their less technologically savvy friends, further reinforcing antisocial behavior. In some cases, individuals move on to programming and destruction of other individuals programs through the writing of computer viruses and Trojan horses; programs which include computer instructions to execute a hacker's attack. If individuals can successfully enter computers via a network, they may be able to impersonate an individual with high level security clearance access to files, modifying or deleting them or introducing computer viruses or Trojan horses. As hackers become more sophisticated, they may begin using sniffers to steal large amounts of confidential information, become involved in burglary of technical manuals, larceny or espionage [6].

The British government released evidence that foreign intelligence agencies, possibly in China, Korea and some former Soviet states, were hacking computers in the United Kingdom. "Economic espionage" was believed to be one reason behind the attacks. Economic espionage involves attempting to undermine the economic activity of other countries, sometimes by passing on stolen industry and trade secrets to friendly or state-owned companies. Key employees; those who have access to sensitive information or government secrets, can be targeted through virus-laden e-mails, infected CD-ROMS or memory sticks, or by hacking their computers. To respond to these threats, the European Union, G8 and many other organizations have set up cybercrime task forces. In the United States, some local law enforcement organizations have electronic crime units and the FBI shares information with these units through its InfraGard program [7].

Cyber security is becoming an important issue, as emphasized in an article by Jacob Silverman titled “Could hackers devastate the U.S. economy?” He discloses the fact that many media organizations and government officials rank it just as grave a threat as terrorist attacks, nuclear proliferation and global warming. With so many commercial, government and private systems connected to the Internet, the concern seems warranted. To add to the concern, consider that today's hackers are more organized and powerful than ever. Many of them work in groups; and networks of black-market sites exist where hackers exchange stolen information and illicit programs. Credit-card data is sold in bulk by "carders" and phishing scams are a growing concern. Malware -- viruses, Trojan horse programs and

worms -- generates more money than the entire computer security industry, according to some experts. He further reveals that hackers are also distributed all over the world, many in countries like Romania that have lots of Internet connectivity and loose enforcement of laws [8].

In 2008 Security experts said Chinese hackers began targeting Western journalists as part of an effort to identify and intimidate their sources and contacts, and to anticipate stories that might damage the reputations of Chinese leaders. In a December 2012 over the course of several investigations it found evidence that Chinese hackers had stolen e-mails, contacts and files from more than 30 journalists and executives at Western news organizations, and had maintained a "short list" of journalists whose accounts they repeatedly attack. Based on a forensic analysis, it appears the hackers broke into *New York Times* computers on Sept. 13, when the reporting for the Wen articles was nearing completion. They set up at least three back doors into users' machines that they used as a digital base camp. From there they snooped around *New York Times'* systems for at least two weeks before they identified the domain controller that contains user names and hashed, or scrambled, passwords for every Times employee [9].

In 2009, dubbed, "Operation: Aurora" by security firm McAfee, sophisticated hackers based in China breached the corporate networks of Google, Yahoo! Juniper Networks, Adobe Systems, and dozens of other prominent technology companies and tried to access their source codes. China's hackers seemed narrowly focused on military technology and telecommunications companies as early as 2000. In 2011 Wiley Rein, a prominent Washington Law firm working on a trade case against China was hacked, and the White House was targeted last year. The hackers also breached the website of the Council on Foreign Relations and rigged it to deliver malware to anyone who visited it. Hacking groups with ties to the Chinese government have also aggressively targeted Western oil and gas companies and their law firms and investment banks [10].

In 2011, U.S. computer security firm McAfee reported that hackers operating from China stole sensitive information from Western oil companies in the United States, Taiwan, Greece and Kazakhstan, beginning in November 2009. Citizen Lab and the SecDev Group discovered computers at embassies and government departments in 103 countries, including the Dalai Lama's office and India, were compromised by an attack originating from servers in China. They dub the network involved "GhostNet". Google claims cyber-attacks from China have hit it and at least 20 other companies. Google shut down its China operations. A top-secret memo by the Canadian Security Intelligence Service warns that cyber-attacks on government, university and industry computers have been

growing "substantially. Quebec provincial police say they dismantled a computer hacking network that targeted unprotected computers around the world, including government computers [11].

In 2011, NASA reported it was the victim of 47 APT attacks, 13 of which successfully compromised Agency computers. In one of the successful attacks, intruders stole user credentials for more than 150 NASA employees – credentials that could have been used to gain unauthorized access to NASA systems. An ongoing investigation of another such attack at Jet Propulsion Laboratories JPL involving Chinese-based Internet protocol (IP) addresses has confirmed that the intruders gained full access to key JPL systems and sensitive user accounts. With full system access the intruders could: (1) modify, copy, or delete sensitive files; (2) add, modify, or delete user accounts for mission-critical JPL systems; (3) upload hacking tools to steal user credentials and compromise other NASA systems; and (4) modify system logs to conceal their actions. In other words, the attackers had full functional control over these networks [12].

NASA is a prestigious target for hackers because of its seat atop the United States' broader technology incubation apparatus, and because of that position it is also a strategic target for foreign state actors and cybercriminals looking to steal information they can profit from. And while the agency reportedly spends about a third of its $1.5 billion IT budget on security, things aren't looking so secure. Securing a huge bureaucracy like NASA is difficult, no doubt. But according to Martin's testimony, as of February 2012 only one percent of NASA's portable devices and laptops were encrypted [12].

According to Bloomberg BusinessWeek, the executive order called for the U.S. Department of Homeland Security to identify which critical infrastructure is vulnerable to a cyber-attack that would be catastrophic to the economy and public safety. According to Apple a week after Obama issued the order, Apple's employees computers were attacked by malicious software after they visited a website aimed at iPhone developers. Shortly afterward Microsoft announced that similar malware has infected some of his company computers. According to trade groups representing tech manufacturers and Web companies, the cables and fibers that information travels over are more critical than the devices and programs their members make, although Tech Companies argue other countries might take a cue from the U.S. and set up their own cyber security guidelines. Multiple sets of regulations might mean manufacturers and Web companies would have to create different products and services for different countries, for further increasing cost [13].

Security experts hired by the New York Times to detect and block the computer attacks gathered digital evidence that Chinese hackers, using methods that some consultants have associated with the Chinese military in the past, breached The Times' network. They broke into the e-mail accounts of its Shanghai bureau chief, David Barboza, who wrote the reports on Mr. Wen's relatives, and Jim Yardley, The Times' South Asia bureau chief in India, who previously worked as bureau chief in Beijing. Security experts found evidence that the hackers stole the corporate passwords for every Times employee and used those to gain access to the personal computers of 53 employees, most of them outside New York Times' newsroom [9].

For three straight years, a group of Chinese hackers waged a cyber-war against a family-owned, eight-person software firm in California, according to court records. It started when Solid Oak Inc. founder Brian Milburn claims he discovered that China was stealing his company's parental filtering software, CYBERsitter. The theft hurt their business and sales, which was bad enough. But twelve days after he publicly accused Chinese hackers, he says he was inundated by attempts to bring down his Santa Barbara-based business. Hackers broke into the company's system, shut down its email and web servers, spied on employees using their own webcams and gained access to sensitive company files, according to court records. Apple Inc. reported it was hacked by the same group that hit social-networking monster Facebook in January 2013. The security breaches are the latest in a string of high-profile attacks on companies including The Wall Street Journal and New York Times. Cyber security firm Mandiant also came out with a report in early 2013 that accused a secret Chinese military unit in Shanghai of years of systematic cyber-espionage against more than 140 U.S. companies. Adam Levin, co-founder and chairman of Identity Theft 911, says that for most companies it's not a matter of if they will have a breach but when Levin told FoxBusiness.com that no company is ultimately immune to this [14].

Members of Congress have published proposals that could result in longer prison sentences for hackers. The House Judiciary committee is looking to expand the Computer Fraud and Abuse Act (CFAA), an anti-hacking bill dating back to 1984. Under the new proposals, damaging a computer after accessing it without authorization would carry a maximum 10-year prison term, double the current punishment. "Trafficking" passwords would also carry a 10-year penalty. Hacking and damaging a "critical infrastructure computer" would become the most serious crime, with a maximum 30-year sentence. That would cover any machine that plays a vital role in areas such as power, transportation, and finance [15].

3.METHODOLOGY

Developing a psychological profile of a likely attacker is an attractive goal. Because of variation among human motivations, and limitations in the knowledge of psychology, such a profile may prove elusive [16]. There are a number of recent and growing trends in the hacking activity landscape that were observed by the Cybercrime division in the past decade dealing with not only the state and local government aspects but with other national governments across the world. Recently, cyber-attacks have no details given to the attackers' identity.

3.1 Data Gathering

In this research study, data was collected from several Department of Justice (DOJ) Cybercrime press releases. However, the bulk of the data was extracted from their department since 2009. DOJ generates reports from cybercrime activity and people across the world. In the United States, more than 35 million dollars in damage has been done to targeted companies. Table 1 consists of 97 hackers listed by nationality, age, job status, reasons for hacking, damage to company, money to judicial system, and punishment from the DOJ for a period of 4 years. A shortlist of hackers is shown in Table 1 as an example. Tables 2 through 4 were constructed from the data collected from the aforementioned references.

Table 1. Computer Cybercrime Portfolio 2009-2013

National	Age	Job Status	Reason for Hacking	Damage to Business	Money to Judicial Sys.	Punish
Sweden	37	N/A	Steal info	N/A	$650,000	Pending
Malaysia	N/A	N/A	Bank fraud	N/A	N/A	10 Y
Romania	N/A	N/A	Steal info	N/A	N/A	7 Y
Russia	55	N/A	Steal info	N/A	$1,000,000	3 Y
America	46	N/A	Personal gain	N/A	N/A	18 Y
America	36	N/A	Destroy company data	N/A	N/A	10 Y
America	49	N/A	Personal gain	$100,000	$250,000	10 Y
America	N/A	Emp	Steal info	$5,000	N/A	40 Y
America	45	N/A	Confidential info	N/A	$1,000,000	15 Y
America	22	N/A	Confidential info	N/A	$350,000	21 Y
America	27	N/A	Personal gain	$9,481.03	$187,659	17 Y
America	28	N/A	Confidential info	N/A	$500,000	5 Y/ 1 Y Pro
Russia	29	N/A	N/A	N/A	$3.5 million dollars	20 Y
Moldova	29	N/A	N/A	N/A		
America	25	N/A	Steal info	N/A	171.6 mil	2Y

Source: U.S. Department of Justice (2009-2012). Computer Crime and Intellectual Property Section Press Releases [17].

Table 2 represents the percentage of the number of hackers by nationality.

Table 2. Hacking by Nationality

Nationality	%	Nationality	%
Unknown	30	Malaysian	2
Russian	3	American	34
Latvian	1	Estonian	11
Romanian	9	Venezuelan	1
Sweden	1	Moldova	1
Albanian	1	Dublin	1
Hungarian	1	Blaine	1

Table 3 indicates the percentage of the type of motivation behind hacking.

Table 3. Motivation behind Hacking

Reasoning	%
Steal Information	34
Intentional Damage to Companies	11
Bank fraud	25
Need employment	1
Personal gain	11
Steal Money	3
Commit Multiple Fraud	7
Steal Intellectual Property	5

Table 4 shows the percentage of the type of penalties applied to hackers by the judicial system.

Table 4. Type of Penalty

Category	%
Pending	42
Probation	3
Supervised release	2
Cyber warfare	15
Prison	41

3.2 Ways to Minimize Potential for Hacking

In order to minimize hacking, several techniques are required. The following procedures need to be implemented to help limit the possibility of hacking:

- ✓ It is quite essential that organizations proactively introduce guidelines of standard use and outline the consequences for inappropriate actions.
- ✓ People should be informed and have adequate knowledge of hacking. They must be educated of certain commonalities and characteristics connected with this activity, as well as the significant penalties for hacking and the repercussions online networking with other characters claiming to be skillful in raiding others.
- ✓ Outside the business perspective, people need to be educated as to not post any sensitive information on social networks such as Facebook, Twitter, YouTube, etc.
- ✓ The organizations can use filters which can prohibit its members from accessing unauthorized software serial numbers, hacking-related materials such as newsgroups, chat-rooms and hacking organizations.
- ✓ Organizational staff should monitor activities in the working environment and be proactive when information is obtained about hacking activities.
- ✓ There is a need for cooperation between private, public, as well as governments to reduce hacking activities.
- ✓ Recognizing good hackers that report vulnerable security weaknesses to companies.
- ✓ Lawmakers need to address the seriousness of cyber hacking by establishing several special centers across the nation where they can recruit the minds of our skilled youth as early as 15 years of age and provide them the proper training, financial means, and support them through college to those who have the passion and commitment to continue in the field of cyber security.
- ✓ Global corporations between nations are needed to reduce hacking.

In summary, people need to be aware of incidents regarding hacking, the mentality associated with it, the consequences of various hacking actions and possible consequences of interacting and forming online relationships with anonymous individuals who claim to be proficient in invading others' privacy. Many organizations have engaged in enabling employees to collaborate with technology-oriented staffs who demonstrate several physiognomies that can result in hacking activities.

4. FINDINGS

The hacking became more serious beyond the extent of individual/groups and it is now at a government level between nations. From the data collected, Tables 2-4 have been analyzed and illustrated as a graphical representation shown in Figure 1-3.

Figure 1 illustrates the number of hacking by nationality. The highest percentage comes from America (35%) and second to it is unknown (31%). Thirdly, it is Estonian (12%).

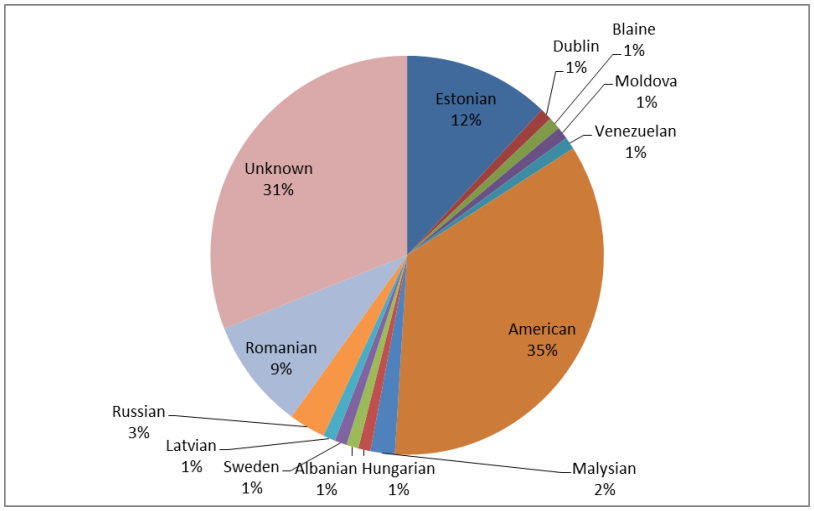

Figure 1. Hacking by Nationality

Figure 2 represents the drive behind hacking; 35% would steal information, 26% is Bank Fraud, and 12% is intentional damage to companies.

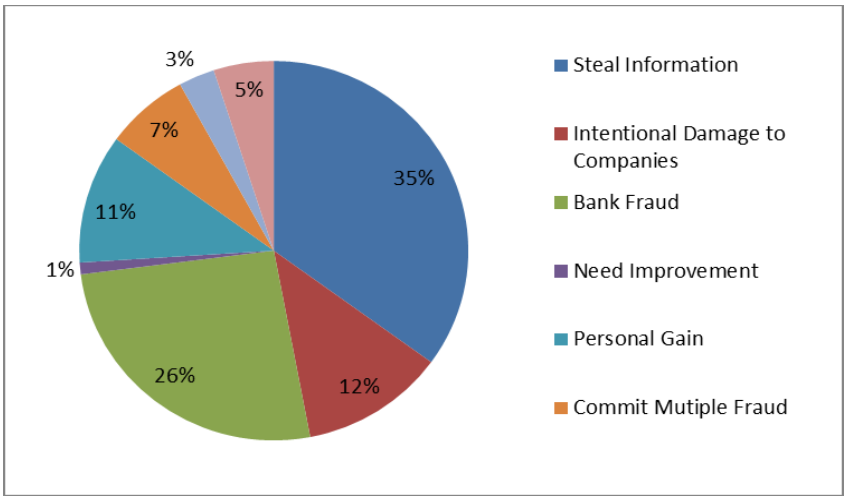

Figure 2. Motivation behind Hacking

Figure 3 shows that 41% of their penalties are still pending which states that their punishments have yet been decided by the courts and 40% are serving a prison sentence. However, 14% are included in cyber warfare which means that their punishment has not been published due to their crime involving the government. Monitoring behavior and motivation of hackers can help improve awareness of their danger and underscores the importance of maintaining robust security, including up-to-date cyber security and anti-virus software.

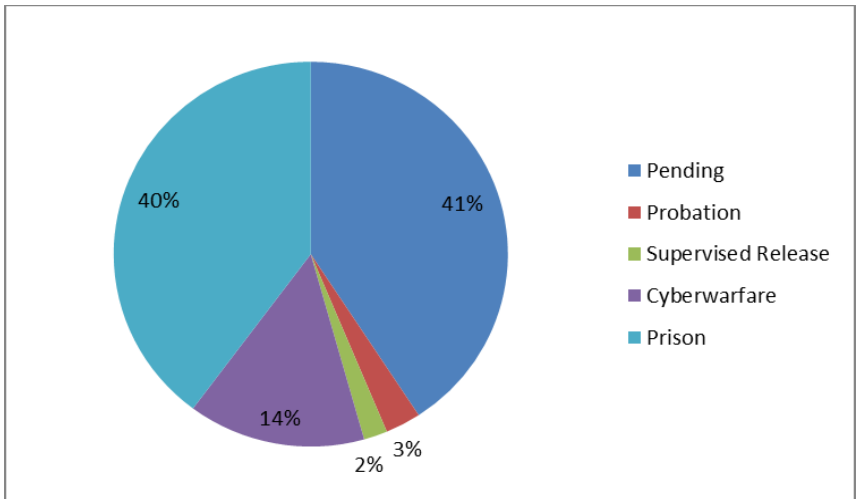

Figure 3. Types of Penalty

Figure 4 shows an example illustrating the seriousness of cyber-attacks in today's society. Chevron, the U.S. headquartered international oil and gas company, has admitted that Stuxnet infected its IT network. Stuxnet is known for destroying centrifuges used in Iran uranium enrichment program. It was designed by a nation state with the intention of targeting Siemens supervisory control and data acquisition systems (SCADA) which controlled the industrial processes inside the enrichment facilities. Industrial Safety and Security Source is reporting that the Stuxnet virus was planted by an Iranian double agent via a memory stick. The Stuxnet malware is widely believed to have caused damage to Iran nuclear program by breaking the motors on 1,000 centrifuges at the Natanz uranium enrichment facility. Kaspersky Lab reported that a new virus dubbed Gauss has attacked computers in the Middle East spying on financial transactions, emails and picking passwords to all kind of pages. The virus resembles Stuxnet and Flame malware which was used to target Iran. Gauss has infected hundreds of personal computers across the Middle East – most of them in Lebanon,

but also in Israel and Palestinian territories. Kaspersky Lab has classified the virus, named after one of its major components, as "a *cyber-espionage toolkit*" [18].

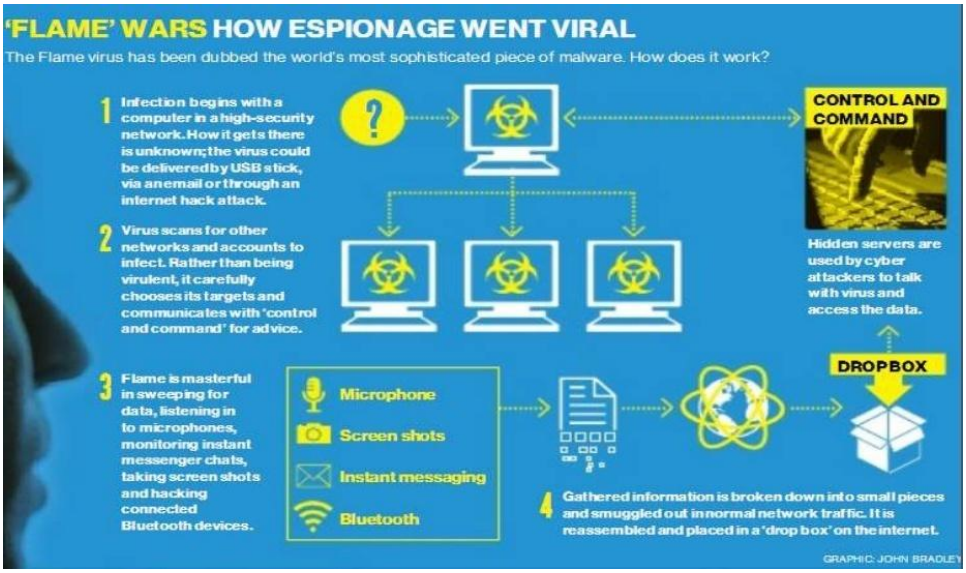

Figure 4. Flame Wars
Source: Cyber Security Helping secure one network at a time, 2013

Recent hacker IT attacks could be catastrophic for global business and even cost lives. According to Alicia Buller [19], the three points to note in cyber war are: Companies could become collateral victims in the war between superpowers. Ideas from state nation cyber weapons could be repurposed and copied by amateurs. Cyber criminals may start using weapons gleaned from governments and nation states. Depending on the severity of the latest hacks, establishing a framework to protect the country becomes top priority of the Obama Administration as well as other countries around the world.

5. CONCLUSION

While computer hackers constitute a major security concern for individuals, businesses, and governments across the globe, hacking and hackers' underground culture remains secretive and difficult to identify for both lawmakers and those vulnerable to hacker attacks. The mystery that surrounds much of hacking prevents us from arriving at definitive solutions to the security problem it poses; but our analysis provides at least tentative insights for dealing with this problem. Hacking became a serious problem affecting all levels of business activities from individuals, corporations, as well as governmental agencies. The bulk of the hacking is initiated from Americans about 35%. The type of penalty ranges from jail time to monetary fines. Although there are laws against hacking, the courts cannot

persecute these crimes fast enough to deter people from committing them. From the literature review, the maximum jail penalty is 62 years and fines are $171.6 million dollars.

Results show that hackers continue to engage in illegal hacking activities despite the perception of severe judicial punishment. A closer look shows that hackers perceive a high utility value from hacking, little informal sanctions, and a low likelihood of punishment. These observations combined with their disengagement from society, partially explains the hacker's illegal behavior. Whatever their reason, it is a learning experience through which they hope to gain anonymity. Future effort to minimize hacking will undoubtedly include a combination of aggressive legislation, new technological solutions, and increased public awareness and education. Existing laws should be reviewed and amended periodically to allow for appropriate evolution. The international community for online security should respond with collaborative efforts globally towards this terrorist act of hacking in order to manage this predicament.

6. REFERENCES

[1] Callwood, K. (2013). "*How to Reduce Hacking*" eHow.com Retrieved from: http://www.ehow.com/how_8663856_reduce-hacking.html#ixzz2Of7JZqMC

[2] Wooten, D. (2009). *"Hacking: modern day threat or hobby? (pt. 1)"*. Retrieved from: http://www.examiner.com/x-13831-Computer-Security-Examiner~y2009m6d22-Hacking-modern-day-threat-or-hobby-pt-1#

[3] Parker, D. (1998). "*Fighting Computer Crime: A New Framework for Protecting Information*" Retrieved from: http://education.illinois.edu/wp/crime/hacking.htm

[4] Shoemaker, D. & Conklin A. (2012). *"Cyber security: The Essential Body of Knowledge 1st edition"* Cengage Learning.

[5] Loganathan, M. & Kirubakaran, E. (2011). *"A Study on Cyber Crimes and protection"* IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1.

[6] Stone, D. (1999). *"Computer Hacking"*, University Laboratory High School, Retrieved from: http://www.ed.uiuc.edu/wp/crime/hacking.htm

[7] Computer Weekly (2006). "*Act on foreign spy risk, firms urged*" Retrieved from: http://www.computerweekly.com/articles/2006/12/01/220307/act-on-foreign-spy-risk firms-urged.htm

[8] Silverman, J. (2007). "*Could hackers devastate the U.S.economy?*" HowStuffWorks.com. Retrieved from: http://computer.howstuffworks.com/die-hard-hacker.htm

[9] Perlroth, N. (2013). "*Hacker in China Attacked the Times for last 4 months*" The New York Times. Retrieved from: http://www.nytimes.com/2013/01/31/technology/chinese- hackers- infiltrate-new-york-times-computers.html?pagewanted=all&_r=0

[10] Canter, D. (2013). "*Fighting an Order to fight cybercrime*" Bloomberg BusinessWeek. March 11-17, 2013.

[11] New Orleans Business News (2011). "*Hackers in China hit Western oil companies, security firm reports*" The Associated Press. Retrieved from: http://www.nola.com/business/index.ssf/2011/02/hackers_in_china_hit_ western_o.html

[12] Dillow, C. (2012). "*In the last year, hackers gained 'Full Functional Control' of NASA networks, stole the control codes for the is*" POPSCI. Retrieved from: http://www.popsci.com/technology/article/2012-03/hackers-gained-full-functional-control-nasa-networks-stole-control-codes-iss-last-year

[13] Engleman, E. (2013). *"Hacked? Who Ya Gonna Call?"* Bloomberg Business Week. February 11- February 17, 2013.

[14] Chakraborty, B. (2013). "*Small firm hit by 3-year hacking campaign puts face on growing cyber problem*" Foxnews.com Retrieved from: http://www.foxnews.com/politics/2013/02/22/small-businesses-big-targets-for-cyber-snoops/#ixzz2Ngj7XMli

[15] Peters, J. (2013). *"America's Awful Computer-Crime Law Might Be Getting a Whole LotWorse"* Retrieved from: http://www.slate.com/blogs/crime/2013/03/25/computer_fraud_and_abuse_act_the_cfaa_america_s_awful_computer_crime_law.html

[16] Stolfo, S. (2008) *"Insider Attack and Cyber Security: Beyond the Hacker"* Vol.39, Springer.

[17] U.S. Department of Justice (2009-2012). Computer Crime and Intellectual Property Section Press Releases. Retrieved from: http://www.justice.gov/criminal/cybercrime/pr.html

[18] Hatcher, W. (2013). "*Cyber Security helping secure one network at a time*" Information Systems Audit and Control Association – Greater New Orleans Chapter – 2013.

[19] Buller, A. (2013). *"The Coming of Cyber War I"* Retrieved from: http://gulfbusiness.com/2013/03/the-coming-of-cyber-world-war-i/