Mahwish Cheema

IT 103, Section 008

2/29/12

The Effect of Computer Hacking on National Security

By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://academicintegrity.gmu.edu/honorcode/ . I am fully aware of the following sections of the Honor Code: Extent of the Honor Code, Responsibility of the Student and Penalty. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://universitypolicy.gmu.edu/1301gen.html web site."

Signature: Mahwish Cheema

Introduction:

The effect of computer hacking on national security is a very pressing issue in today's time especially because each generation is becoming more and more adept in using advanced technology. Everyday technology is progressing and because of this we have to be aware of computer hackers. "A computer hacker is a person who finds out weaknesses in the computer and exploits it." ("Hacker", 2012). These hackers have threatened national security by hacking into governmental records and have even initiated animosity between countries ("French Finance Ministry Suffers Cyber-attack", 2011). The specific purpose of this paper is to inform the audience that the effect of hacking on national security greatly impacts nations in negative ways.

Background:

Hackers may use security exploits in order to achieve their intended effect of hurting a nation. "A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice" ("Hacker", 2012). As described, these security exploits are tools that hackers can use to penetrate national security systems. According to Klimburg (2011), hacking is often sponsored by non-governmental agencies to exploit nations. This goes against the notion that countries initiate cyber warfare themselves. Next, this paper will discuss the potential benefits of hacking national security.

Potential Benefits:

When it comes to hacking national security, there is really no benefit for anyone except the hacker. The nation will risk losing its stability by being hacked or the people of the nation may lose their personal information to a hacker. According to Rubin (2012), a "pro-Israeli

hacker" put the Facebook emails' and passwords' of 30,000 "helpless Arabs" on a hacking website. This exemplifies the fact that there are benefits for the hacker such as fulfilling his/her selfish and political motivations by making other people of a nation miserable. The Arabs who were hacked felt attacked not just individually, but as a whole Arab nation against the Israeli hacker. This one hacker caused everyone anger and an obstruction of trust.

According to Cooney (2009) "The Central Intelligence Agency…anticipates growing cyber threats as a more technically competent generation enters the ranks." As Cooney (2009) says, since the CIA is expecting cyber hacking to occur, they are prepared for the worst. This can be looked at as a potential benefit because nations are improving their own security systems to avoid hackers. Similarly, "The growing number of cyber threats has led to increased demand for cyber security experts certified in IT master's degree, penetration testing, computer forensics, security audit, ethical hacking and security analysis" ("French Finance Ministry Suffers Cyber-attack", 2011). The popularity of the new cyber security field is so extreme because of these harmful hackers. Now, it is important to examine the legal and ethical issues of hacking national security.

Legal and Ethical Issues:

There are numerous legal issues involved with hacking national security information. According to Cooney (2009), "Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community." Some hackers do not even hack for their own monetary gain like expected, but simply break the law just to get "bragging rights". Stealing national intelligence and personal information is illegal. If the hackers were caught, severe consequences would follow. According to Klimburg (2011), "Chinese and Russian hackers have been behind a significant number of high-profile and hostile cyber attacks on a

number of countries." Because these hackers are so inconspicuous it is hard to pinpoint the exact people who did the hacking. If countries were to make laws and punishments greater for hackers perhaps less hacking would take place.

Hackers also break ethics. It is morally unjustified to steal information. According to Rubin (2012), "Now, after roughly 10 decades of actual physical fighting between Palestinian Arabs (and their brethren) and Jews, the struggle has moved to the electronic battlefield. In fact, in recent weeks there have been a host of serious clashes that have threatened not just soldiers, but every single citizen in the Middle East." In this situation we can see that both sides have fallen short of being ethical and now it is just full on cyber attacking for both the Jews and Palestinians. Next, it is vital to observe security concerns.

Security Concerns:

The largest problem when it comes to security concerns in regards to hacking national security is that often times individual data and information becomes available for the public to see. Cooney (2009) says "[hackers] damage public morale and confidence". He is absolutely right, because the hacker not only stole their information, but also their assurance. Also, the loss of national, confidential documents is a huge issue to discuss. "Cybercriminals intruded into around 150 computer systems at the Ministry and gained unauthorized access to several confidential documents." ("French Finance Ministry Suffers Cyber-attack", 2011). The French Finance Ministry lost many top secret papers due to the fact of hackers stealing and intruding information. Hacking all in all is a security concern. Hacking interferes with the normal route of cyber traffic and causes negativity on all ends. To follow the analysis further, now this paper will examine social problems.

Social Problems:

Within the realm of hacking national security, many social problems such as trust issues do arise. Hackers sometimes end up representing a group of people or a "nation". According to Rubin (2012) the "pro-Israeli Hacker" ended up representing the Jewish population and the "helpless Arabs" represented the Muslim population. One hacker caused two huge groups of people to get into frenzy with one another. Israel vs. Palestine is already a touchy subject to most of these people affected, and bringing it up in the context of cyber-war is really painful for some. This hacker caused thousands of people to get angry at one another and even raised the hostility between Muslims and Jews (Rubin 2012). To further understanding of this topic, it is important to look at further required research.

Further Required Research:

In order to have an even better grasp on hacking national security it is necessary to do more research. Further research that will be useful to this topic should come from credible sources such as the ProQuest Database. By going even deeper into the material, more knowledge will be learned because there will be more facts and examples to back up every idea formed. Further required research is definitely not an option, it is a necessary step to take in order to reach a high knowledge competence.

Conclusion:

The central idea of this paper was that hacking into national security has major negative consequences. There are not enough benefits to hacking to make it an "okay" practice. It is illegal and unethical to hack national records because of the chaos that would follow. Also, there are many security concerns due to the fact that hacking can make private information become public information. There are social concerns as well when it comes to hacking on a national

level because it can cause hatred between two countries or two groups of people. You should never take your privacy for granted, you are a part of a nation; if the nation is attacked by hackers, your private information could be at risk.

Reference Page

Michael Cooney. (2009, November). The six greatest threats to US cybersecurity: Cybersecurity threats from government insiders, forgieng countries, terrorists all pose grave threats, GAO reports.. Network World (Online). p. 1. Retrieved March 1, 2012, from Proquest Computing. (Document ID:1906257311). http://proquest.umi.com.mutex.gmu.edu/pqdweb?index=9&did=1906257311&SrchMode=2&sid=2&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1330572194&clientId=31810

This *trade publication* is a credible source because it comes from a well noted author. This source is also a trade publication so it gives me a variety when using sources. This source is also credible because I found it on the ProQuest Database through GMU's Library. This source was valuable to me because it really discussed the core of being a terrorist/hacker.

French Finance Ministry Suffers Cyber-attack. (8 March). *M2 Presswire*, p.1. Retrieved March 1, 2012, from ProQuest Computing. (Document ID: 2285715911). http://proquest.umi.com.mutex.gmu.edu/pqdweb?index=4&did=2285715911&SrchMode=2&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1330572164&clientId=31810

This *website* was a credible source because I found it on the ProQuest Database. Also, M2 Presswire is a famous news line that has received praise in the past. This source was valuable to me because it gave me a really great example of hacking into France's national security.

Rubin, N.. (2012, January). Hacking Wars. Baltimore Jewish Times, 324(3), 12. Retrieved March 1, 2012, from ProQuest Religion. (Document ID: 2585917251). http://proquest.umi.com.mutex.gmu.edu/pqdweb?index=0&did=2585917251&SrchMode=2&sid=2&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1330572070&clientId=31810

This *magazine* is credible because it came from the ProQuest Database. Also, this Baltimore Jewish Times magazine is a well-known magazine so it is more credible. It was a valuable source to me because it gave a great example of Israel and Palestine and how a cyber-conflict caused both nations to become agitated.

Klimburg, A.. (2011). Mobilising Cyber Power. *Survival, 53*(1), 41. Retrieved March 1, 2012, from Social Science Module. (Document ID: 2344603191). http://proquest.umi.com.mutex.gmu.edu/pqdweb?index=0&did=2344603191&SrchMode=2&sid=2&Fmt=2&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1330572015&clientId=31810

This *scholarly journal* is credible because a scholar wrote it and it is from the ProQuest Database. This source was valuable to me because there were lots of facts in this article that helped me form some arguments.

Hacker (computer security). (2012, February 28). Wikipedia. Retrieved March 1, 2012. http://en.wikipedia.org/wiki/Hacker_(computer_security)#Security_exploits

This *webpage of Wikipedia* is credible because many people have edited it and there are official citations that come from journals to support all the claims on the page. This source really

helped me with the definition of computer hacking.