Jordan M. Lee

Term Paper – Stuxnet

Professor Jones

6 May 2020

CIS-211

**Introduction**

The National Security Agency (NSA), Central Intelligence Agency (CIA), U.S. Strategic Command (USSC), and the Israeli Defense Force (IDF) Unit 8200 were the brains behind one of the most aggressive cyber-attacks ever seen called Stuxnet. This topic holds great significance in the computer industry because it was the first time a computer virus was used in a cyber warfare attack on a country. Attention was drawn to the computer malware after it concluded its mission because after it was finished the computer malware started to replicate in the wild (public internet domain).

The term “wild” refers to the malware being released into the public domain along with the source code. More attention needs to be drawn to Stuxnet because the cyberattack was significant in terms of the level of complexity and mission. The computer malware (Stuxnet) is important to analyze because it took multiple U.S. government agencies and an ally of the U.S. to develop the code for the malware. It is also significant to analyze how Stuxnet was able to sabotage the centrifuges in the Iranian facility.

**Background Information**

Understanding how Stuxnet became the world’s first cyberattack dates back to the 1950s. Iran (then) was an ally to the United States and the U.S. gave Iran technical training along with an experimental nuclear reactor that was small in size. The goal for Iran was to develop a nuclear energy program and during that period, they were receiving aid from the U.S. until the revolution happened in 1979.

Concerns were coming from the UN (United Nations) in terms of Iran having possible nuclear capabilities. Since Iran and Israel are neighboring countries, Israel had great concerns about Iran potentially having nuclear weapons. Israel expressed its concerns to the U.S. and both countries shared the concerns, but the U.S. was in no position to intervene. Israel would then go on to try and sabotage Iran’s nuclear campaign.

A screenshot of a cell phone

Description automatically generated

Stuxnet infected hosts by country in 2010 (source: Statista)

**Literature Review**

Israel started to destroy and sabotage nuclear materials and equipment being shipped to nuclear facilities in Iran. Israel went to great lengths to eliminate Iran’s nuclear program which included bribing and even assassinating Iranian engineers and scientists. The United States eventually joined Israel to assist in eliminating Iran’s nuclear program in terms of sabotage and intercepting shipments of equipment and bringing them back to U.S. facilities in the region. According to Sanger (2012) “For years, the C.I.A. had introduced faulty parts and designs into Iran’s systems – even tinkering with imported power supplies so that they would blow up – but the sabotage had relatively little effect”.

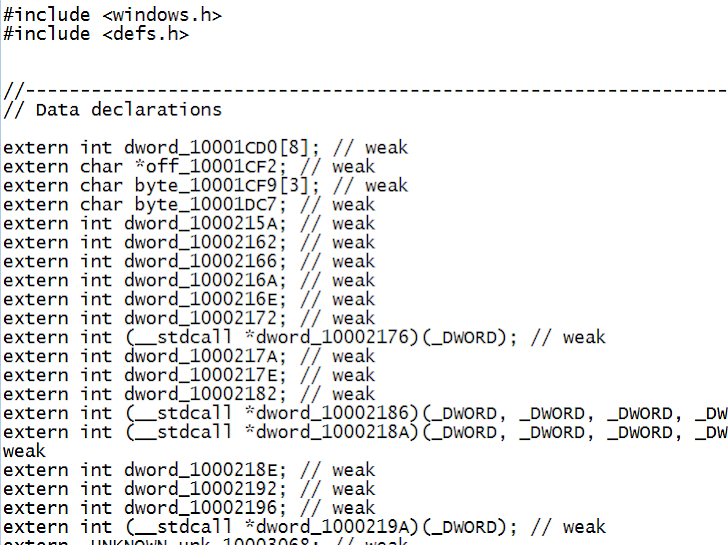
* Viewing the situation from Israel’s point of view; I would not want my neighbor firing off nuclear missiles when I live next door. The United States got dragged into the mix because the U.S. and Israel are allies, so that meant that when Israel started the campaign against Iran the U.S. had to join. Iran wanted to restart its nuclear program, so it outsourced to China, Russia, and Pakistan for assistance with supplies and training.
* That led to the United Nations placing sanctions on Iran which also led the U.N. to find out that Iran had secret facilities capable of producing nuclear weapons. In my opinion, in terms of the United States and Israel trying to sabotage Iran’s nuclear program I would agree. Analyzing the situation, I agree because Iran was considered a hostile state and during that time they threatened an ally country of the United States and they needed to be stopped.

In 2006, when George W. Bush was president, he was faced with the problem of going to war with Iran over the nuclear program or allowing the completion of the program. Stephen Hadley was the national security advisor and Condoleezza Rice was the secretary of state during Bush’s presidency and he tasked them to find him another option. It was General James E. Cartwright of the U.S. Strategic Command who presented the option of using a cyber weapon. According to Sanger (2012) “General James E. Cartwright, who had established a small cyber operation inside the United States Strategic Command, which is responsible for many of America’s nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.”U.S. Strategic Command spearheaded the operation, but it was the NSA who developed the actual cyberweapon that was going to be used. The plan was that the use of the cyberweapon would allow time so the sanctions that were being placed on Iran would work. In an article written by Nakashima and Warrick (2012), “Olympic Games became a collaborative effort among NSA, the CIA, and Israel, current and former officials said. The CIA, under then-Director Michael V. Hayden, lent its covert operation authority to the program.”

* In my opinion from a technological point of view, I agree that the use of Stuxnet was ethical to use. I say this because the Iranian population was not in any immediate danger, the population was not threatened by another country trying to start a war and invade their country. I can apply the consequence-based ethical theory to this situation because it supports my argument.
* The consequence-based ethical theory explains how utilitarians argue that the outcome or consequences for the greater good of society are paramount in decision-making. In terms of the theory, the outcome of the malware was done in terms of the greater good for the population of the U.S. and Israel.

Code-named “Olympic Games” Stuxnet the computer malware was created. According to Nakashima and Warrick (2012) “Code-named Olympic Games, said it was first developed during the George W. Bush administration and was geared towards damaging Iran’s nuclear capability”**.** Even though this was a joint cyber operation with Israel the NSA rap point on this. The goal of Stuxnet was to penetrate the computer networks of Iran’s most secure nuclear facilities and destroy the enrichment centrifuges through electronic sabotage. The computer code or source code was also written to gain access to the industrial computer controls at the Natanz Nuclear Plant. The computer code was written to target these hardware devices called PLCs or programmable logic controllers that Iran was using to control the centrifuges in the facility. In the same article written by Nakashima and Warrick, they stated: “The use of the cyberweapon – malware designed to infiltrate and damage systems run by computers – was supposed to make the Iranians think that their engineers were incapable of running an enrichment facility”.

* In my opinion, I agree with the tactics that Israel and the U.S. used to penetrate and destroy Iran’s nuclear centrifuges. I believe that it was the operation was a great success because Stuxnet completed the mission. As I mentioned before the use of a cyber weapon caused no harm to the Iranian population.
* It’s a simple fact that the U.S. and Israel had the technological capability to write a malicious computer code that was able to complete the mission without having to use military force. Warrick and Nakashima mentioned a great point in their article about how Stuxnet made the engineers of Iran seem incapable of operating the Natanz plant.



Stuxnet Malicious Code Snapshot

(Source: The Hacker News)

To achieve the goal of sabotaging the computer systems, the Olympic Games acted in stages. The first stage was the beacon, the beacon was inserted into the computer networks at the Natanz plant and other facilities. The beacon was essentially a piece of computer malware. The entire cyber attack was highly sophisticated, but the first stage was the most critical because the beacon was used to recreate the electrical structure of the Natanz plant. This blueprint would be used to understand how the centrifuges were connected inside the plant which allowed the NSA and IDF to analyze the complexities of the electrical circuits. The blueprint was the roadmap needed to understand how the Natanz plant operated. In an article written by David E. Sanger (2012), he stated that “The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds”.

Once the beacon was inserted into the computer networks, it would then send messages back to NSA headquarters. The messages would describe in great detail the normal day-to-day operations and security details at the enrichment facilities. One of the network security features the Natanz plant used was “air gapping”. Air-gapping is a security measure that ensures a secure computer network is physically disconnected from unsecured networks like the public internet or any unsecured LAN networks. In the same article written by David E. Sanger (2012), he mentioned that “Mr. Bush was skeptical, but lacking other options, he authorized the effort”.

* Analyzing the situation, I agree with former President Bush to authorize the use of Stuxnet. I say this because President Bush was put in a highly stressful situation and didn’t have many options. Even though this was the first time a cyberweapon would be used as an offensive cyberattack, this still was the best option offered.
* In my opinion, the beacon stage was the most critical part of the entire mission; it was the roadmap for the entire operation because it allowed the NSA to analyze the internal network of the Natanz facility. It would take some time for the beacons to work and report all the data back to the NSA with a complete diagram of the electrical grid as it pertains to how the centrifuges were interconnected.



Iran’s Nuclear Enrichment Facility (Natanz Plant)

(Source: Sarbakhshian/Associated Press)

At this point in the operation, Stuxnet’s beacon was relaying data back to the NSA and CIA who were analyzing the data to understand the layout of the facility. The second stage was that a new version of the beacon (computer malware) was developed. It was then reinserted into the Iranian computer network where it would again sit in the background and monitor the normal day-to-day activity of the facility before being activated. In terms of complexity in regards to the computer malware code, this is where the IDF Unit 8200 assisted the NSA. When Stuxnet was green-lighted it was able to relay back to Iranian engineers what appeared to be normal activity at the facility, but at the same time, the computer network was being compromised and infected with the computer malware. To Iranian engineers, on their end, it would appear that all operations and proceedings were happening without errors, but that wasn’t the case. Since the goal of Stuxnet was to delay Iran’s nuclear program, Stuxnet was written to never attack in the same manner twice which is what left Iranian scientists confused.

According to David E. Sanger (2012) “Then the NSA and a secret Israeli unit respected by American Intelligence officials for its cyber skills set to work developing the enormously complex computer worm that would become the attacker from within”.That sentence from Sanger explains that the NSA needed help from an ally developing computer malware. It also explains how complex it was to write the code to make the malware and that our (U.S.) Israeli counterparts are highly respected and qualified to deliver. The reason the Olympic Games was successful was that the Israeli IDF had extensive knowledge and intelligence about the operations going on at the Natanz plant. It was this intelligence that the NSA wanted that brought both intelligence agencies together.

* I agree with the decision of the NSA to collaborate with the Israeli IDF to gather more intelligence and develop computer malware. In my opinion, I would do the same because Israel had more knowledge of what was going on inside the facility. As I have mentioned Stuxnet was targeting Windows systems and devices called PLC which are considered a type of SCADA system.

Stuxnet started development under President Bush and then continued its development into President Obama's term. It’s the fact that Stuxnet was so ingeniously developed that President Bush wanted to see if it would work. Once Stuxnet was fully developed it needed to be tested. David E. Sanger (2012) mentions that “The United States began building replicas of Iran’s P-1 centrifuges, an aging unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market”.

The U.S. military and intelligence officials involved with testing the Olympic Games had developed a virtual replica of the Natanz nuclear plant. The test ran for several months with great success, the computer malware successfully destroyed the centrifuges by making them spin out of control until they were destroyed. After all the testing was concluded, senior National Security advisors dumped some of the wreckage of the test on the desk in the situation room for President Bush to view. This was the proof needed to green-light the operation to show that the test was indeed successful. Once President Bush saw the wreckage he immediately approved the Olympic Games and declared it ready to be used on the actual target.

* In my opinion, I believe that President Bush made the right decision to authorize the Olympic Games into action after he saw what the cyber weapon was capable of doing. In my research, I found it interesting how history works because if the U.S. didn’t have access to P-1centrifuges that they recovered from the Libyan dictator Muammar el-Qaddafi I believe that the testing phase would have delayed the entire operation.

I mentioned the term ‘air-gapping’ already but this concept is the most common practice for governments and militaries to use to secure their computer networks. The Iranian network was never connected to the internet, so the tricky part of the entire operation was how would the virus get into the facility. Israeli IDF intelligence was very critical because Israel had the most knowledge of Iranian engineers and facilities. The U.S. and Israel composed a list of Iranian engineers, scientists, maintenance workers, and people. Both countries created the list with two key qualities; Iranian engineers and scientists who have physical access to enrichment facilities and poor computer security habits.

The engineers, scientists, and maintenance workers were both spies or just unwitting accomplices. The way the computer malware got into the computer network at the enrichment facilities was with the use of a thumb drive (flash drive). Davis E. Sanger (2012) writes “In fact, thumb drives turned out to be critical in spreading the first version of the variants of the computer worm; later more, sophisticated methods were developed to deliver the malicious code.”The thumb drives were infected over the internet, so when the engineers and scientists went to plug the flash drives into the secure network, Stuxnet would freely jump back and forth allowing the NSA and Israeli IDF to have two-way access to the network. According to Atika Shubert (2011), “Stuxnet infected a third party first, likely a trusted contractor to the Natanz facility”.

In 2008 the first set of centrifuges started to spin out of control and the Iranians had no idea as to what was causing the malfunction. Like I mentioned before Stuxnet was designed to never attack in the same fashion twice so that’s what confused Iranian engineers and scientists the most. They had no idea as to what was attacking their internal computer network system. It has been said that Iran began to become so distrustful of each other that the International Atomic Energy Agency (IAEA) had to be sent into some enrichment facilities to keep watch of what was occurring inside.

President Obama came into office with cyber issues on his agenda. The architects of Stuxnet would meet Obama in the situation room and present him with a folder that contained highly classified information regarding Stuxnet. The folder contained a schematic diagram of Iran’s nuclear production facility. President Obama continued to authorize the attacks and would receive updates every few weeks and also authorize the next steps.

* I want to mention how critical Israel was in the operation because, without their inside intelligence, the U.S. would have been at a complete disadvantage. Also, I'm not sure how much influence the U.S. when it came to persuading the Iranian engineers and scientists to commit espionage on their own country. I would think that Israel had significant influence because the two countries are neighboring.
* It amazes me that Stuxnet was so sophisticated that it drew top engineers and scientists up the wall. I agree with President Obama’s decision to continue using the Olympic Games to dismantle Iran’s nuclear program. In my opinion, the program needed to continue because of the way Stuxnet was designed. It was designed to not attack in the same manner twice, so that meant it was designed to have multiple attacks and it would attack in different waves.

I want to mention again when I stated that once Stuxnet completed its mission the computer malware started to replicate in the public domain of the World Wide Web (WWW). The Olympic Games began operating in 2006 and lasted up until 2010. The Stuxnet computer worm started to unexpectedly replicate across the public internet infecting many computers globally. Although Stuxnet was quoted to be “harmless” it was designed to only attack certain parameters inside a nuclear facility, it only operated in the environment of attacking Iranian nuclear facilities.

The most damaging thing about the Olympic Games being released in the wild was that the source code was made public to anyone who wanted to look through to see how it was developed. David E. Sanger (2012) mentions “But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage.” Stuxnet escaped because of an error in the computer code which was then able to spread to an engineer’s computer. Sanger (2012) “When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed.”

The engineer working at the Natanz facility had no clue that his computer became the host computer for the world’s first cyberweapon from which the computer malware would start replicating. With Stuxnet self-replicating in the public domain and with people having access to the source code, they were able to trace the origins. From a political point of view, the U.S. and Israel did not take responsibility for the attack and both countries used plausible deniability. The U.S. at the time believed that it was a modification error done by the Israeli, but was never confirmed by officials familiar with the matter.

* When Stuxnet started replicating itself in the public domain it caused a huge problem for both governments of Israel and the U.S. because the computer malware was never intended to be released in the public internet domain and it was not developed to self-replicate. In my opinion, all secret missions/operations come to light at some point in time, so for the Olympic Games, that time came in 2010. The computer security company Symantec got ahold of the source code and started to take an in-depth look at what the Stuxnet computer malware was.
* The codename “Olympic Games” was the official name of the entire operation, but when the malware became active in the public domain it was given the name Stuxnet. I also want to mention how much of a political game this was for Israel and the U.S. because the entire idea of the operation was to delay Iran from producing nuclear reactors so that the sanctions that the U.N. placed on Iran could work. Stuxnet was just a delaying tactic and for the most part, completed its mission.

**Conclusion**

In conclusion, Stuxnet, or Olympic Games is single-handily the most aggressive cyberweapon ever used to date! Stuxnet was a piece of computer malware that crippled an entire nation's nuclear program by electronically sabotaging their equipment. In terms of complexity, the virus was developed by allied countries. Multiple agencies including the NSA, CIA, and U.S. Strategic Command played a key role in maintaining, developing, and securing the computer code and overall operational secrecy. The Israeli IDF Unit 8200 was tasked with assisting the NSA and CIA to develop the code for the Olympic Games. Without the Olympic Games being developed I believe that Iran would have been able to produce nuclear weapons that would have threatened Israel’s national security and potentially started another conflict in the Middle East.

**References**

Singer, P. W. (2015). Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons. Case Western Reserve Journal of International Law, 47(3), 79–86

Blewett, D. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon. Library Journal, 139(18), 104

Prince, B. (2012). New Book Claims President Obama Ordered Stuxnet Attack on Iran. EWeek, 6

Nakashima, E., & Warrick, J. (2012, June 02). Stuxnet was the work of U.S. and Israeli experts, officials say. Retrieved September 15, 2016, from [https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U\_story.html?noredirect=on&utm\_term=.50d33930f261](about:blank)

Zetter, K. (2017, June 03). The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks. Retrieved September 15, 2016, from [https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/](about:blank)

Sanger, D. E. (2012, June 1). Obama Order Sped Up Wave of Cyberattacks Against Iran. Retrieved February 9, 2020, from [https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html](about:blank)

Statista Research Department. (2010, November 30). Stuxnet - the percentage of infected hosts by country. Retrieved March 3, 2020, from [https://www.statista.com/statistics/271110/stuxnet-infected-hosts-by-country/](about:blank)

Shubert, Atika. “Cyber Warfare: A Different Way to Attack Iran's Reactors.” *CNN*, Cable News Network, 8 Nov. 2011, [www.cnn.com/2011/11/08/tech/iran-stuxnet/index.html](about:blank).

Zetter, K. (2017, June 4). Stuxnet Missing Link Found, Resolves Some Mysteries Around the Cyberweapon. Retrieved from [https://www.wired.com/2013/02/new-stuxnet-variant-found/](about:blank)