The History of Stuxnet:

Key Takeaways for Cyber Decision Makers

Military Category

Cyber Conflict Studies Association - Call for Papers

June 4th, 2012

History is the witness that testifies to the passing of time; it illuminates reality, vitalizes memory, provides guidance in daily life and brings us tidings of antiquity. — Cicero

Introduction

In each profession and aspect of daily life there are decision makers who guide from their area of influence. These decision makers exist at every level of civilian and military leadership. It is through their choices, and the understanding of their choices' impacts, that a nation collectively moves forward. This forward movement also exists in the development of the cyberspace domain. Cyber decision makers dictate tactical and strategic level choices to include capability development, employment, and overall strategies. It is by these choices that the cyberspace domain acts as a national level projection of power. The projection of power through offensive and defensive strategies in cyberspace offers unique challenges compared to the other warfighting domains due to its comparative youth. As a relatively new domain it is imperative to understand the history of key cyber events so that modern day decision makers can capitalize on the lessons learned. It is in this way that the best choices for the vectoring of the domain will present themselves.

The Stuxnet cyber attack on the Iranian nuclear enrichment facility at Natanz is seen by many as the first true cyber weapon.[1] This makes Stuxnet's importance as a cyber event unparalleled in modern cyber history and specifically worth understanding. Lessons learned from the Stuxnet cyber attack enable intelligence and cyberspace professionals, as cyber decision makers, to better operate within the domain. This paper will explore the history of the Stuxnet

1. John P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (2011): 23-40.

cyber attack and three key takeaways from the attack. These three takeaways are:

- Cyber attacks may be linked and can offer warnings of future threats
- Cyber attacks can confirm or reveal new attack vectors and tactics
- Speculative attribution can affect political tension and cyber deterrence

The Iranian Nuclear Program

In properly understanding Stuxnet and its implications it is beneficial to have a brief understanding of the history behind the Iranian nuclear program. Following the 1945 use of the nuclear bombs "Little Boy" and "Fat Man" on the Japanese cities of Hiroshima and Nagasaki, respectively, the United States launched a program known as Atoms for Peace.[2] The Atoms for Peace program was an initiative launched by President Eisenhower. One of the program's many goals was to discourage the development and employment of nuclear weapons while establishing the United States a premier nuclear power.[3] On March 5th, 1957 Iran's Shah Mohammad Reza Shah Pahlavi entered into an agreement with the United States under the Atoms for Peace program for the "proposed agreement for cooperation in research in the peaceful uses of atomic energy.[4]"

Over the course of the next twenty years Iran moved forward with its goals for nuclear power plants. The Tehran Nuclear Research Center (TRNC) was founded in 1967 and supplied with a 5-megawatt nuclear research reactor from the United States. The reactor was known as

---

2. "How Iran Went Nuclear," *New Statesman,* June 22, 2009, 26.

3. Sam Roe, "An Atomic Threat Made in America," *Chicago Tribune,* January 28, 2007, accessed May 26, 2012, http://www.chicagotribune.com/news/nationworld/chi-061209atoms-day1-story,0,2034260.htmlstory.

4. Greg Bruno, "Iran's Nuclear Program," *Council on Foreign Relations,* March 10, 2010, accessed May 26, 2012, http://www.cfr.org/iran/irans-nuclear-program/p16811.

the Tehran Research Reactor (TRR) and consumed highly enriched uranium as a fuel source.[5] An important part of the agreement for Iran to receive nuclear support from the United States was the signing of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). This was signed by Iran in 1968 and opened Iran's nuclear program to inspection by the International Atomic Energy Agency (IAEA).[6]

It is important to note that these steps forward for Iran marked the nation as a modern power and was a point of pride for Iran's government. The Shah wanted to further expand the program by making plans for an additional twenty-three nuclear power stations. The goal was to have these additional stations operational by 2000 as there were concerns that oil reserves would become limited.[7] To achieve this goal, agreements had to be made with corporations to include the German company Kraftwerk Union AG. In 1975 Iran signed a contract with Kraftwerk Union AG, a joint venture between Siemens AG and Allgemeine Elektrizitäts-Gesellschaft (AEG), worth between $4-$6 billion USD. The contract outlined the details for a nuclear power plant that would house two 1,196 MWe pressurized water reactors to be completed by 1981.[8] In the midst of the Iranians' plans there was growing tension over the true purpose of the nuclear power plants. The Deputy Chief of Mission at the US Embassy in Tehran, Jack Miklos, expressed issues with the plans due to an inability of Iranian officials to explain how Iran would

---

5. "Tehran Nuclear Research Center," *The Institute for Science and International Security*, accessed May 26, 2012, http://www.isisnucleariran.org/sites/facilities/tehran-research-reactor-trr/.

6. Greg Bruno, "Iran's Nuclear Program."

7. Sam Sasan Shoamanesh, "History Brief: Timeline of US-Iran Relations until the Obama Administration," *MIT International Review*, accessed May 26, 2012, http://web.mit.edu/mitir/2009/online/us-iran-2.pdf.

8. Henry U. Ufomba and Robert O. Dode, "Which Way to Tehran? Pre-emptive Air Strike Cumulative Diplomacy, Technical Isolation and the Iranian Nuclear Crises," *Journal of Public Administration and Policy Research* 2, (2010): 46-52.

use their desired 23,000 MWe of additional power over the next twenty years; there simply was not a need for that much energy.[9] Jack Miklos felt that the desire was in part to keep a nuclear option open to Iran should other regional nations achieve nuclear capabilities. His concerns were solidified when the Shah made comments that Iran would leave options open and be prepared to create nuclear weapons if other currently non-nuclear nations did the same.[10] The Shah's statements were due largely in part to a 1974 Indian nuclear test. The 1974 nuclear test, known as Operation Smiling Buddha, was the first nuclear test explosion from a nation that was not one of the five permanent members of the United Nations Security Council.[11]

The United States decided that additional agreements and constraints on the Iranian nuclear program were needed to include a multinational reprocessing facility. Iran felt that the US policy was overly restrictive and expressed concerns of having foreign surveillance in their facilities. Despite these concerns, a deal was signed in March 1978 under President Carter that allowed the US to veto the reprocessing of spent nuclear fuel.[12] The agreement caused tension in Iran amongst government officials who felt the Shah had catered too largely to the desires of the West. In 1979 everything changed for the nation's nuclear program.

The Iranian revolution in 1979 concluded with the overthrow of the Shah and his replacement with Ayatollah Ruhollah Khomeini. The new Islamic republic caused additional concerns to the West regarding the state of the Iranian nuclear program. Over the next few years the agreements between Iran and various corporations, including Kraftwerk Union AG, were

---

9. William Burr, "A Brief History of US-Iranian Nuclear Negotiations," *Bulletin of the Atomic Scientists,* 65, no. 1 (2009): 21-34.

10. Ibid.

11. "Smiling Buddha: 1974," last modified November 8, 2001. http://nuclearweaponarchive.org/India/IndiaSmiling.html.

12. William Burr, "A Brief History of US-Iranian Nuclear Negotiations."

largely considered null and void with no refund of money paid to the Iranian government.[13] Additionally, Iran found it challenging to gain support for building nuclear power plants. Yet, in the 1990s Iran entered into an agreement with Russia to gain Russian experts and technical information regarding nuclear power. In 1995 Iran signed a contract with Russia to finish the Bushehr plant with a 915 MWe pressurized water reactor.[14]

In addition to the Bushehr plant, Iran had also been working on bringing an underground facility at Natanz into operation. In 2002, a dissident group known as the National Council of Resistance of Iran revealed the existence of the uranium enrichment facility at Natanz.[15] Tension between Iran and the West grew to an all-time high in 2006 when Iranian President Mahmoud Ahmadinejad confirmed that Iran had completed its goal of enriching uranium. The announcement was met with strong backlash from a number of countries including the United States. President George W. Bush stated that the rising threat from the Iranian government, in regards to the enriching of uranium, must be met with strong consequences.[16] The United States was most vocal in denouncing the Iranian government's decisions to continue with enriching uranium but it was only one of many nations watching Iran closely. Sometime around President Ahmadinejad's announcement in 2006 there was at least one nation-state secretly working on an answer to the Iranian nuclear program. The secretly crafted reply would not publically surface until June 2010.

---

13. Ibid.

14. Adam Tarock, "Iran's Nuclear Programme and the West," *Third World Quarterly* 27, no. 4 (2006): 645-664.

15. Greg Bruno, "Iran's Nuclear program."

16. President George W. Bush, "President Bush Addresses American Legion National Convention," *The White House*, August, 2006, accessed May 26, 2012, http://georgewbush-whitehouse.archives.gov/news/releases/2006/08/20060831-1.html.

Enter Stuxnet

On June 17th 2010, security researchers at the Belarus security firm VirusBlokAda received reports of a new piece of malware. An Iranian customer contacted VirusBlokAda after experiencing continuous and unintentional reboots on a SIMATIC WinCC server.[17] WinCC is a program created by Siemens and written on the Microsoft Windows operating system. The program acts as a human-machine interface (HMI) for operating and modifying programmable logic controllers (PLCs). Control systems and their components, including PLCs, are present in a wide variety of locations. Control systems automate and monitor systems in industries ranging from oil refining, satellite communication, the power grid, water filtration, and nuclear enrichment.[18]

In examining the new malware, VirusBlockAda researchers identified a potential Windows zero-day, or previously unpatched vulnerability. Given the severity of a zero-day vulnerability, the security firm decided to email and notify researchers at Microsoft. Researchers at Microsoft started working on analyzing the malware's 1Mb of binary code to identify and remedy the vulnerability. To put the difficulty of this task into perspective, the 1Mb code was twenty times larger than most other malware. The researchers reverse engineered the binary code into a form that could be read and interpreted by them; overall the code was incredibly complex.[19]

Through their research the team identified four Windows zero-day vulnerabilities, an

---

17. Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair,* April 2011, accessed May 28, 2012, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

18. Joe Weiss (leading control systems cyber security expert), telephone interview by author, June 2, 2012.

19. Bruce Dang, "Adventures in Analyzing Stuxnet," (presentation at 27th Chaos Communication Congress, Berlin, Germany, December 27-30, 2010).

unprecedented amount for malware, affecting a variety of Windows operating systems including XP, Vista, and Windows 7.[20] These exploits allowed the malware to quickly exploit a Windows system and self-propagate throughout a network while gaining administrator level privileges on the system. An interesting aspect to the researchers was that some of the exploits used against the vulnerabilities were fairly simple. Although the code was advanced and complex, the exploits were more akin to tricks which used the built in functionality of the operating system against itself. However, these functions of the system were so unknown that many of the Microsoft team members did not even know they existed.[21] This high level of understanding of the systems infected would become a common theme in the malware to be known as Stuxnet.

The Stuxnet worm, a worm is a piece of malware that can self-propagate throughout a network, was named for file extensions found within its code. It quickly became heavily analyzed by numerous security researchers and companies. Analysis on Stuxnet revealed that beyond the four zero-day exploits there were a number of other advanced features including a Windows rootkit, a distributed command and control network, the ability to peer-to-peer update, legitimate signed digital certificates, and various antivirus evasion techniques.[22] The rootkit allowed Stuxnet to reintroduce itself to an infected system after the system was cleaned of the malware. The command and control network allowed the creators and operators of the malware to remotely access it, give it commands, and update it. The peer-to-peer updating built into Stuxnet allowed it to update and communicate with itself even when separated from the

---

20. Ibid.
21. Ibid.
22. Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier,"*Symantec Security Response*, last modified February, 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

command and control server or an Internet connection. The signed digital certificates allowed the malware to install a driver on systems without prompting the user. This driver was the launching point for Stuxnet to install its encrypted libraries of code onto an infected system.[23] The features identified made Stuxnet an incredibly advanced piece of malware, but they were only one portion of the code.

Stuxnet was split into two sections identified as the weapon system and the payload. The weapon system portion of the worm enabled the malware to infect systems and spread throughout the network utilizing the zero-day vulnerabilities. Once Stuxnet was on a system it would check to make sure very specific parameters were met before initiating its payload.[24] In particular, Stuxnet would only initiate its payload on specific Siemens Process Control System (PCS) 7 controllers. If Stuxnet identified itself on any other system it would simply do nothing. In addition to being precise, the payload placed the first ever PLC rootkit on the controllers for persistent access.[25] The payload portion of the code was the purpose behind infecting the systems and what truly makes Stuxnet a cyber weapon instead of just an advanced piece of malware.

Through extensive analysis, it was identified that the controllers that Stuxnet initiates its payload on are located at the Natanz uranium enrichment facility in Iran. Analyzing the code alone was not enough to prove this though as the schematics and layout of the Natanz facility are sensitive and secret in nature. However, the President of Iran visited the Natanz facility which provided a photo opportunity for use on his official website. Unknowingly to him, the photo

---

23. Ibid.
24. Ibid.
25. Ibid.

captured a portion of a screen which currently displayed the layout of the facility.[26] Stuxnet expert Ralph Langner caught this mistake and compared it to the Stuxnet code. It was a perfect match.[27]

The payload was specifically crafted to target the gas centrifuges at the Natanz facility and leverage a number of checks and attack sequences against the targets. Stuxnet would check the system it was on to ensure that it was a gas centrifuge controller in the Natanz facility, run modules in its code to check the current settings and time on the device, decide if the settings and conditions were appropriate for an attack, and if everything matched perfectly it would spin the centrifuges faster than they were intended to go before slowing them back down again. The specific speed the centrifuge would speed up to, 1410 Hz, is the maximum degradation point for the type of centrifuges used at Natanz and would have required extensive knowledge on the devices to know.[28]

The creators of the Stuxnet worm would have also had to have intimate knowledge of the Natanz facility prior to launching an attack so that the payload would initiate properly without any guidance from a command and control network. This means that the attackers either had insider knowledge of the facility or mapped it out with another cyber asset. In either case it demonstrated a level of understanding, dedication, and an espionage campaign that rivaled any other ever orchestrated in the cyberspace domain. In addition, to know exactly how the PLCs would function under the payload's code and instructions, the creators would have been a few of

---

26. "Visit to Natanz Facility," *2011 Presidency of the Islamic Republic of Iran,* April 8, 2008, last accessed May 28, 2012, http://www.president.ir/en/9172.

27. Ralph Langner, "Stuxnet: A Deep Dive*,"* (presentation at Digital Bond's SCADA Security Scientific Symposium, Miami, Florida, January 19-20, 2012).

28. Ibid.

the best PLC programmers in the world. The payload was extremely precise and demonstrated a level of knowledge past that which even the operators at the facility would have had.[29]

Analysis of the exploits used in Stuxnet showed that the likely initial infection of the Natanz facility took place via a universal serial bus (USB) device. It is unknown whether the initial infection was the result of infecting a drive that was used by an unknowing participant or instead implanted on purpose by a double agent.[30] Analysis of the malware showed that however it was planted onto the Iranian network it was done at least as early as June, 2009.[31] This minimum of a year in operation is consistent with the attack routines in Stuxnet's code. The payload was designed to slowly degrade the centrifuges over an extended period of time. This attempt to cause damage over a period of time instead of quickly damaging as much as possible indicates that the attackers wanted to have the worm remain hidden.[32]

Due to the highly secretive nature of the Natanz facility in Iran, the true timeline and impacts of Stuxnet are unknown. Experts believe that the malware was likely in development and being tested around 2007 with its initial infections on the Iranian network taking place no later than 2009.[33] At first though, the Iranian government claimed that there was no infection. When the Stuxnet infection was acknowledged, the government stated that there was no damage caused by Stuxnet. However, on 29 November, 2010 President of Iran Mahmoud Ahmadinejad

---

29. Ralph Langner (leading Stuxnet expert), discussion with author, 11th Control System Cyber Security Conference, Washington DC, October 17-21, 2011.

30. Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet.Dossier."

31. Ibid.

32. Ralph Langner, "Stuxnet: A Deep Dive."

33. Elizabeth Montalbano, "Stuxnet, Duqu Date Back to 2007, Research Says," *Information Week*, December 29, 2011, accessed May 29, 2012. http://www.informationweek.com/news/security/vulnerabilities/232301131.

admitted that Stuxnet had infected Iranian nuclear facilities and disrupted the program by targeting facility centrifuges.[34] Satellite photography and investigation from the IAEA has indicated that at least 1,000 centrifuges, of the 9,000 present at Natanz, were damaged beyond repair as a result of the Stuxnet infection.[35]

The Stuxnet cyber attack was not only one of the most advanced pieces of malware ever launched but also the first known to result in the destruction of physical infrastructure outside of a controlled test environment. The protection of critical infrastructure has been a national point of concern dating back to May 22nd, 1998 when The White House published a directive aimed at the growing vulnerabilities to critical infrastructure.[36] It was not until Stuxnet though that this style of attack was publically demonstrated. The implications of the attack were powerful and pushed a number of security vendors, researchers, and control systems experts to look more heavily into the defense of these systems.

Security experts knew that if a secret nuclear facility was prone to an attack then so were the other industries that used control systems. This public realization led to many security researchers and computer hackers testing exploits and attack methods against control systems.[37] In addition, Stuxnet showed that attacks in the cyberspace domain could be as destructive and

---

34. William Yong and Robert F. Worth, "Bombing Hit Atomic Experts in Iran Streets," *The New York Times*, November 29, 2010, accessed May 29, 2012, http://www.nytimes.com/2010/11/30/world/middleeast/30tehran.html?_r=2&hp.

35. David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security*, December 22, 2010, accessed May 28, 2012, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/#2.

36. "Presidential Decision Directive/NSC-63," *The White House*, May 22, 1998.

37. Gerry Smith, "Cyber-Crimes Pose 'Existential' Threat, FBI Warns," *Huffington Post*, January 1, 2012, accessed May 28, 2012. http://www.huffingtonpost.com/2012/01/12/cyber-threats_n_1202026.html.

precise as those carried out in the traditional domains of warfare.

Takeaway #1: Cyber Attacks May Be Linked and Can Offer Warnings of Future Threats

One of the more interesting lessons learned from Stuxnet was that an advanced cyber attack may be linked to other pieces of malware. Specifically, multiple pieces of malware can be built from the same coding framework and be used for very different purposes. This allows the attack team to quickly update their malware, adapt it for unique targets, and use different pieces of malware together in either direct or indirect support of each other. Consequently, pieces of malware that are linked can give hints to cyber defenders on what the malware creators may be working on next.

On October 14th, 2011 a new malware was identified and named Duqu for a common file extension found in its code.[38] The piece of malware was quickly noted as being related to Stuxnet as the two shared a large portion of the same source code and similar features.[39] Initially, some security vendors' systems mistakenly identified the new malware as actually being Stuxnet.[40] However, the two pieces of malware are very different in various aspects and their intended purposes.

To infect a system with Duqu, the attackers would send a phishing email to an intended target. Inside the email was a Microsoft Word document that when opened would initiate a

---

38. "W32.Duqu," *Symantec Security Response*, last modified November 23, 2011, last accessed May 28, 2012, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_Duqu_the_precursor_to_the_next_stuxnet.pdf.

39. Based off of original analysis performed on Stuxnet and Duqu by the author, Jeremy Sparks, and Paul Brandau in conjunction with analysis performed by Matthew Weeks.

40. Mikko Hypponen, "Duqu – Stuxnet 2," *F-Secure*, October 18, 2011, accessed May 29, 2012, http://www.f-secure.com/weblog/archives/00002255.html.

Microsoft Windows zero-day exploit. Instead of four zero-days as were found in Stuxnet, Duqu only used one zero-day which was an exploit based on a vulnerability in Microsoft Word fonts.[41] The Duqu creators also showed a bit of humor with how they infected target systems. One of the phishing emails was sent from "Mr. B. Jason," presumably representing the fictional spy in the "Bourne Identity" series, Jason Bourne. In addition, the Microsoft Word font was named Dexter, which is the name of a television show about a serial killer who only kills bad people. The font included a copyright statement for Showtime who owns the rights to Dexter.[42]

Once the weapon system portion of the code infected a system, the exploit gave administrative rights directly to the malware so that it could initiate its payload. The payload would install its files and open a connection back to a command and control server at one of three locations. The command and control servers were located in Belgium, India, and Vietnam and provided a varied and redundant method for communication with the malware.[43] The attack team could then control the malware to locate and export sensitive files as well as install a keylogger to capture system key strokes. The captured information and files were encrypted and packed into an image file before being sent to a command and control server.[44] Duqu's intended purpose of capturing information is entirely different than the purpose of Stuxnet. The larger variance though comes in the style differences displayed in the two cyber attacks.

---

41. Vikram Thakur, "Duqu: Status Updates Including Installer with Zero-Day Exploit Found," last updated November 3, 2011, accessed May 29, 2012, http://www.symantec.com/connect/w32-Duqu_status-updates_installer-zero-day-exploit.

42. Alexander Gostev, "The Duqu Saga Continues: Enter Mr. B. Jason and TV's Dexter," *Securelist*, November 11, 2011, accessed May 29, 2012, http://www.securelist.com/en/blog/208193243/The_Duqu_Saga_Continues_Enter_Mr_B_Jason_and_TVs_Dexter.

43. "W32.Duqu," *Symantec Security Response*.

44. Ibid.

Stuxnet was a worm that spread quickly through any Windows system it came across without prejudice. Estimates of Stuxnet infections reach well into 100,000 with locations in Iran, India, Europe, and the United States.[45] In contrast to this rapid infection style, Duqu was set to only infect its intended targets and was designed as a remote access trojan (RAT). RAT styled malware have been used in targeted cyber attacks before with the specific purpose of cyber espionage.[46] The fact that Duqu did not spread like Stuxnet made it stealthier and more difficult to detect.

To make Duqu even stealthier the creation team built in a kill function. After thirty-six days of operating on a target the malware would delete itself completely from the system.[47] This feature made detecting and analyzing Duqu incredibly difficult for security researchers. As a result, very few instances of the malware's payload currently exist to be examined and even fewer copies of the weapon system portion of the code have been obtained. This in itself offers network defenders and attack teams pros and cons on different styles of infection and sustainment of cyber attacks.

The locations infected with Duqu offered clues as to what kinds of information its creators were interested in. The targets included research laboratories, manufacturing plants, and certificate authorities in Europe, India, Iran, Sudan, and Vietnam.[48] Analysis done on the targets and style of Duqu indicated that this type of cyber espionage would be needed to create a piece

---

45. Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, March/April 2012, accessed May 29, 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,3.

46. Dmitri Alperovitch, "Revealed: Operation Shady RAT," *McAfee*, accessed May 29, 2012, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

47. Ryan Naraine, "Duqu FAQ," *Securelist*, October 19, 2011, accessed May 29, 2012, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

48. Ibid.

of malware like Stuxnet. The information gathering malware could capture schematics of a facility to be attacked, steal digital certificates used in installing the malware's payload, and gain other critical information such as what defense systems are in place at the target location.[49]

It is currently unknown as to whether Duqu was used to create Stuxnet or if it was created to develop the next Stuxnet styled cyber attack. However, on March 20, 2012 a new instance of Duqu was discovered with an updated encryption algorithm to aid in evading detection.[50] This new variant of the malware showed that the team behind Duqu is still active in their operation and looking for additional sensitive information. By understanding the link between Stuxnet and Duqu, the fact that Duqu is still active offers clues to network defenders. There would be no reason to continue the Duqu operation if an additional attack was not in production or already underway. Additionally, the link between Duqu and Stuxnet shows that the malware creation team is willing to continue attacks using a common platform.

The link between the two pieces of malware is their use of shared source code through a coding platform known as Tilded.[51] The platform was identified December 29, 2011 and named Tilded due to the proclivity of "~d" as a file extension in the code. The coding platform itself was focused on the driver used to install the encrypted files of Stuxnet and Duqu.[52] Tilded

---

49. Guilherme Venere and Peter Szor, "The Day of the Golden Jackal – The Next Tale in the Stuxnet Files: Duqu Updated," *McAfee Labs*, October 18, 2011, accessed May 29, 2012, http://blogs.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal-%E2%80%93-further-tales-of-the-stuxnet-files.

50. Greg Masters, "Duqu Variant Uncovered," *SC Magazine*, March 23, 2012, accessed May 29, 2012, http://www.scmagazine.com/duqu-variant-uncovered/article/233385/.

51. Alexander Gostev, "Stuxnet/Duqu: The Evolution of Drivers," *Securelist*, December 28, 2011, accessed May 29, 2012, http://www.securelist.com/en/analysis/204792208/Stuxnet_Duqu_The_Evolution_of_Drivers.

52. Ibid.

provided a base for the malware and an ability to use different modules in creating Stuxnet and Duqu.

By using different modules of code the malware creators could modify, remove, or add modules to make entirely different pieces of malware as demonstrated with Stuxnet and Duqu. This module and platform based approach has been likened to a Lego set where a large number of different malware can exist from the same base platform.[53] This approach to malware is not unique in Tilded but is a high profile example of it used in an advanced cyber attack. Cyber decision makers can benefit from understanding this link between Duqu and Stuxnet as it provides an example of a proven weapon development and employment strategy. Furthermore, in understanding this link additional threats can be identified, seen as working together, and countered appropriately.

Takeaway #2: Cyber Attacks Can Confirm or Reveal New Attack Vectors and Threats

Stuxnet's use of the Tilded platform and its link to Duqu offer a number of lessons learned to cyber decision makers. One of those lessons is that the tactics, techniques, and procedures demonstrated by cyber attacks are available to anyone once the cyber weapon is employed. In addition, the technologies and exploits utilized by Stuxnet provided a public framework for executing future attacks. An original cyber attack may be the product of genius level and innovative development but analysis of the malware and its lessons learned provide a much more easily replicated attack.

The Tilded platform demonstrates the epitome of an efficient cyber attack. This platform

---

53. Jim Finkle, "Stuxnet Weapon has at Least 4 Cousins," *Reuters*, December 28, 2011, accessed May 29, 2012, http://www.reuters.com/article/2011/12/28/us-cybersecurity-stuxnet-idUSTRE7BR1EV20111228.

showed that a common base could be created and then adapted for different outcomes and operations. As a nation-state built cyber weapon, the Tilded platform offered its creators a certain level of project secrecy and time critical options. Nation-state weapons, regardless of type, require oversight and approval processes. In the case of a cyber attack two of the most important resources are time and secrecy.

If the target changes, updates defense systems, or unknown variables come into play the chances for a cyber operation to succeed are drastically reduced. However, by having an already approved cyber platform, changes to the weapon's payload can be made without requiring the same level of approval that would be required through initiating a new project. This is similar to how a military aircraft can change payloads dictated by mission requirements instead of designing an all new aircraft. In the case of cyber weapons, not having to initiate new projects, teams, or gain new approval for the same type of mission keeps less people in the know about the operation. This operational secrecy is critical to a cyber weapon as once the details of the weapon are known they are much more easily countered. The streamlined process of a single project also reduces the amount of time required for the attack to take place.

The ability to update code and change out payloads on a cyber weapon capitalizes on the resource of time and better enables operational success. Many current defense systems rely on signature based detection to defeat malware. As malware is identified and analyzed, a signature is built for sensors and programs so that when it is detected trying to enter a system it can be blocked. This is most commonly seen in home user antivirus programs. When a piece of malware updates its code though it does not match the signature built and thus can infect systems relying on that defense again. The Tilded platform style of attack makes signature based detection useless in protecting critical assets.

In non-signature based defense systems, advanced cyber attacks may be met with more complex challenges. The Natanz facility's internal network is not connected to an outbound Internet connection. This process of network separation, known as an air gap, provides additional levels of defense against malware.[54] The malware must find a way to infect an air gapped network and then to carry out its intended purpose without the benefit of a command and control server. In the case of Stuxnet, the malware had a very specific purpose that needed the highest level of targeting parameters met for the operation to succeed. Once it was on the network, the attack team behind Stuxnet also needed an ability to update the malware if any changes were required. This was crucial as many unknown variables exist in a remote target such as Natanz and would require the attack team to adapt Stuxnet to overcome them.

To defeat the air gap, Stuxnet remained hidden on a USB device until it was plugged into a Windows system. This allowed the malware to transcend the need for an Internet connection and infect the separated network. Once on the network, Stuxnet used its peer-to-peer feature to receive additional instructions, updates, or a kill function if it had been needed.[55] When Stuxnet connected to another system that was already infected, it would check the versions of the malware against each other. The systems running older versions of Stuxnet would update themselves from the newest versions.[56] In this way the team behind Stuxnet could introduce an update to any system at Natanz and feel confident that it would propagate and update properly throughout the entire network. During the course of the Stuxnet operation there were at least

---

54. Lukas Milevski, "Stuxnet and Strategy: A Space Operation in Cyberspace," *Joint Forces Quarterly*, 63, no. 4 (2011): 64-69.

55. Ibid.

56. Liam O Murchu, "Stuxnet P2P Component," *Symantec*, September 17, 2010, accessed May 29, 2012, http://www.symantec.com/connect/blogs/stuxnet-p2p-component.

three different variants identified.[57]

The strategy behind Stuxnet demonstrated that the team behind the attack pulled the best aspects from previous malware and devised a highly effective plan. This strategy is now one that any other cyber attack team can learn from and copy. In this way there were risks associated with Stuxnet. Once launched, it provided an effective strategy for infiltrating and targeting critical infrastructure of any nation, even the nation that created Stuxnet. In addition, the vulnerabilities that Stuxnet exploited are now known to everyone who wishes to exploit them as well. Although patches are available for most of the vulnerabilities, systems must be updated with the patches to defend against the attacks. This does not always happen though and thus many systems are still vulnerable to Stuxnet and attacks using its exploits. Stuxnet itself utilized a vulnerability, not counted as one of the four zero-days, that had been identified at the beginning of 2009 with a patch widely available.

In the beginning of 2009 the malware known as Conficker, a worm that infected millions of computers in over 200 countries, exploited a vulnerability identified as MS08-067.[58] This particular vulnerability allowed Conficker, and likewise Stuxnet, to spread quickly through networks. The team behind Stuxnet likely learned from Conficker and updated their code with an exploit for this vulnerability.[59] In this same manner, other pieces of malware can learn from the vulnerabilities of Stuxnet and update their code appropriately. This has already been seen in

---

57. Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier."

58. John Markoff, "Defying Experts, Rogue Computer Code Still Lurks," *The New York Times*, August 26, 2009, accessed May 31, 2012, http://www.nytimes.com/2009/08/27/technology/27compute.html.

59. Alexander Gostev, "Myrtus and Guava, Episode MS10-061," *Securelist*, September 14, 2011, accessed May 31, 2012, http://www.securelist.com/en/blog/2291/Myrtus_and_Guava_Episode_MS10_061.

the newly identified Flame malware.

Flame, discovered 28 May 2012, is a complex malware designed for a cyber espionage campaign against targets in the Middle East including Palestine and Iran.[60] Much like Duqu, the malware infects highly targeted systems and gathers information to send back to command and control servers. Unlike Duqu, Flame is large, 20Mb in size, and captures a much wider variety of information including systems configuration settings, audio communication, and Skype conversations.[61] Interestingly, Flame utilizes the same vulnerability to spread via USB devices that Stuxnet used. Malware experts believe that the similarities in Flame and Stuxnet indicate that they may have been written by the same nation-state but different teams within the organization.[62] Regardless of who wrote Flame, the evidence shows that its creation team learned from Stuxnet.

Routine patching to limit what malware creators can use from each other is not always possible. Specifically in the case of control systems and critical infrastructure it can be one of the hardest defenses to properly maintain. Control systems and critical infrastructure generally operate customized versions of software in unique settings. When a patch becomes available for those systems it must be tested out thoroughly before it is introduced to the control systems environment. Without proper testing, a patch may have unintended consequences and

---

60. sKyWIper Analysis Team, "sKyWIper (a.k.a. Flame a.k.a. Flamer): A Complex Malware for Targeted Attacks," *Laboratory of Cryptography and System Security*, last updated May 31, 2012, accessed May 31, 2012, http://www.crysys.hu/skywiper/skywiper.pdf.

61. Ibid.

62. Nicole Perlroth, "Researchers Find Clues in Malware," *The New York Times*, May 30, 2012, accessed May 31, 2012, http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

cause damage to an environment or cause it to break down altogether.[63] Some of the control systems currently in operation have not been stopped for years and to restart them would be a challenge that many organizations cannot currently face.[64] Stuxnet thus demonstrated that attacks against control systems and critical infrastructure are viable long after they are discovered. In addition, Stuxnet demonstrated that not all vulnerabilities identified will be fixed.

Beyond the four zero-day vulnerabilities that Stuxnet exploited in its weapon system, there were additional vulnerabilities in the payload portion of the code. One of the vulnerabilities was that the default setting for the PLCs operating the gas centrifuges at Natanz was to allow automatic read and write capability on the controller.[65] This is the equivalent of having default administrator access. However, the controller's manufacturer did not view this as a vulnerability and instead identified it as a feature. For this reason, the features that Stuxnet exploited in its payload, to inject malicious code onto the PLCs, will not be changed. Stuxnet thus identified an attack vector useful against controllers across the world that any other piece of malware can be still be designed to take advantage of in an attack.

The code portion of Stuxnet that took advantage of this read and write feature in the controllers was very basic yet demonstrated expert knowledge. The ability to inject code in a controller was particularly useful to Stuxnet because it allowed the safety controls on the systems to be turned off.[66] With the safety features disabled, the controllers allowed Stuxnet to spin the centrifuges fast enough to break. This would have normally been noticed by the Natanz facility

---

63. Joe Weiss, telephone interview by author.

64. This was information gathered from a variety of presentations that the author attended at the 11th Control Systems Cyber Security Conference, Washington DC, October 17-21, 2011.

65. Ralph Langner, "Stuxnet: A Deep Dive."

66. Ibid.

operators which would have aided them in detecting Stuxnet. To remedy this, Stuxnet took advantage of another aspect of the systems without technically exploiting a vulnerability.

After infecting the facility operators' WinCC systems and modifying the controllers, Stuxnet acted as a man-in-the-middle style attack. Instead of relaying error messages to the operators' systems, Stuxnet would loop back facility display settings previous to the attack. When the engineers looked at the computers monitoring the centrifuges everything appeared to be operating normally.[67] Without proper feedback from the systems, the Natanz facility members could not understand why the centrifuges were breaking. Until Stuxnet was identified in 2010, numerous Iranian scientists were fired because the Iranian government assumed either incompetence or sabotage on behalf of the operators.[68] This added to the overall stealth and psychological aspects of the Stuxnet cyber attack.

Features, vulnerabilities, and strategies identified in Stuxnet and other cyber attacks are incredibly useful in the creation of other malware. The lessons learned are also useful in defending against the attacks. For example, the ability to inject read and write code on a controller, as Stuxnet did, identified a method of bypassing safety features at control systems across the world. Disabling or tampering with safety features in control systems can result in the direct loss of human life. It is imperative to learn from cyber attacks such as Stuxnet and apply the information to the security of networks and critical assets as well as the creation of cyber weapons that operate ethically.

Takeaway #3: Speculative Attribution can Affect Political Tension and Cyber Deterrence

One of the first mysteries surrounding the Stuxnet cyber attack was that of attribution.

---

67. Joe Weiss, telephone interview by author.
68. Ibid.

No nation-state or organization claimed the attack on the Natanz uranium enrichment facility in Iran. There was no use of traditional forces or military strikes like those demonstrated by Russian forces following the cyber attacks on Georgia in August, 2008.[69] The cyber attack on Natanz successfully delayed the Iranian nuclear program for at least a year and demonstrated the power of a nation-state grade cyber weapon; there was no need for any additional forces. Without any nation taking credit for Stuxnet, researchers turned to the code and looked for any clues that may have been left behind. The speculated attribution applied to Stuxnet served as a case study for the difficulty of attributing cyber attacks and what kind of impacts that attribution, whether it is accurate or not, can have.

Inside the Stuxnet code there were two clues left behind that seemed to indict Israel as a creator of Stuxnet. The first was a series of numbers, 19790509. The numbers read like a date and possibly represent May 9th, 1979. The news media took the discovery of the date and credited it as a reference to the execution of Habib Elghanian who was a Jewish Iranian living in Tehran.[70] The death of Habib Elghanian was one of the first civilian executions by the Islamic Iranian government following the 1979 Iranian revolution. Due to the execution, around 100,000 members of the Jewish community in Iran left the country.[71] This led to the creation of theories and news articles that the numbers were left by an Israeli coder as a statement of revenge placed inside of Stuxnet.

The second clue left behind in the Stuxnet code was a reference to "Myrtus." Myrtus

---

69. John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 12, 2008, accessed May 31, 2012, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

70. Larry Seltzer, "Symantec Puts 'Stuxnet' Malware Under the Knife," *PC Mag*, October 1, 2010, accessed May 31, 2012, http://www.pcmag.com/article2/0,2817,2370107,00.asp.

71. Ibid.

may simply stand for "My RTUs." A remote terminal unit is abbreviated as "RTU" and is commonly found in control systems. However, Myrtus may also be used as a reference to the Book of Esther in the Bible's Old Testament.[72] This again points to a possible Israeli connection as in the Book of Esther the Jewish forces discover a Persian attack plan and successfully wage a preemptive attack. The combination of Myrtus and 19790509 with the motivation of Israel to deny Iran nuclear weapons caused the focus of attribution to be placed on them. However, the coding styles of the weapon system and payload portions of Stuxnet are different and indicated that there was a second nation-state involved.

One of the largest supporters of Israel has been the United States. With their shared desire to keep nuclear weapons out of the hands of the Iranian government, the United States seemed like the perfect choice for creating Stuxnet. The United States also possessed the technical expertise and kind of budget that would have been required to create the advanced malware. Strengthening the theory, another piece of evidence that surfaced was a project in 2008 where the Idaho National Laboratory partnered with Siemens to help secure their Step 7 software. This software runs in conjunction with the Siemens Process Control System (PCS) 7 controllers.[73] The PCS 7 controller was the same type that was targeted at Natanz. Access to Step 7 software source code by some of the world's best engineers seemed to attribute the creation of Stuxnet's payload to the United States.

The theories continued that the United States likely created the payload portion of the

---

72. Ibid.

73. Jeffrey Carr, "Idaho National Lab: Homeland Security or Homeland Conspiracy?" *Forbes*, January 20, 2011, accessed May 31, 2012, http://www.forbes.com/sites/jeffreycarr/2011/01/20/idaho-national-lab-homeland-security-or-homeland-conspiracy/.

Stuxnet code and tested it out on P-1 centrifuges, similar to those used at Natanz. The centrifuges were obtained after Libya gave up its nuclear program in 2003.[74] The centrifuges were supposedly located at Oak Ridge National Laboratory in Tennessee, which is under the Department of Energy with Idaho National Laboratory. In addition, news organizations believed that Israel likely tested the cyber weapon at their secret Dimona complex.[75]

These pieces of evidence have been followed with numerous statements from unnamed sources that the United States and Israel teamed together to create and deploy Stuxnet. A book that came out in June 2012 claimed that sources from inside President Obama's Situation Room, among others, confirmed the United States' involvement in Stuxnet with Israel under code name Olympic Games.[76] The book states that Stuxnet began development in 2006 under President Bush and continued its operation under the direction of President Obama. The mysteries of Stuxnet may not ever be completely satisfied but the latest development, if accurate, ties many of the theories together. The impacts of this attribution though are not determined by the validity of the evidence but by the speculation itself.

The speculative attribution applied to Israel and the United States over the last two years has shown that unnamed sources, small pieces of evidence, and motive can be used to convince an international community of nation-state involvement in a cyber attack. This has powerful

---

74. William J. Borad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 15, 2011, accessed May 31, 2012, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

75. Ibid.

76. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, accessed June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

implications not only to the difficult task of attributing a cyber attack but also to the political strain placed on nation-states that are accused of participating in such an attack.

Following the Stuxnet cyber attack political tensions between Israel, the United States, and Iran increased drastically. Iran stated that they were creating a new cyber police unit to monitor their networks and that they would be establishing a cyber warfare unit. Brigadier Gen. Gholamreza Jalali, leader of the Iranian Passive Defense Organization, stated that their mission would be "to fight our enemies with abundant power in cyberspace and Internet warfare.[77]" As Iran tried to recover from both the physical damage and embarrassment of Stuxnet it was unclear if they would seek reprisal for the attack. If Iran had saw Stuxnet as an act of war and wished to retaliate the targets would have been the United States and Israel.

The United States government has stated that cyber attacks against the United States can be viewed as acts of war which would warrant a military response.[78] If an attack similar to Stuxnet was carried out against the United States and pieces of evidence as mundane as dates and references were purposely left in the code, it could influence a war with a nation that may have not been involved. Leaving false attribution and trails of evidence is not difficult to do with malware. Although there is plenty of evidence pointing to an Israeli and United States connection to Stuxnet, many of the pieces of evidence could have been easily placed by a third nation. Whether or not this happened in Stuxnet is not the issue, the concern is that it is possible in future cyber attacks. This real world socio-political tension created between the people and governments of nation-states could lead to disastrous outcomes.

---

77. Ibid.

78. Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, May 30, 2011, accessed June 1, 2012, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

As a result of the attribution applied to the United States and Israel there was also an effect on cyber deterrence. The issue with creating cyber deterrence, as opposed to deterrence in the traditional domains of warfare, is that cyber weapons are not displayed. In many cases cyber weapons remain secretive projects known only to their creators. Without the ability to showcase weapons and capabilities, true deterrence cannot be generated. Nation-states may believe their enemies to not possess the ability to retaliate or attribute cyber attacks and thus the nation appears weak to that form of warfare. By not displaying cyber capabilities, there is a small level of deterrence between nation-states created in that nations may assume other governments have better capabilities than they actually have. In the same way though, a nation-state may inaccurately assume itself superior to another. Stuxnet left no doubt that a pair of nation-states possessed unprecedented cyberpower.

While the United States and Israel may have suffered political tensions through speculated attribution applied to them, they also gained a level of credibility and cyber deterrence. The very public demonstration of cyberpower resulting in the physical destruction of secretive critical infrastructure assets sent a strong message. The nation-states responsible, presumably the United States and Israel, not only had the capability to successfully launch the advanced operation but also the willingness. It is impossible to directly measure cyber deterrence but it was undoubtedly affected by Stuxnet. The best measure of deterrence may be that there has not been any successful retaliation on the United States and Israel for the Stuxnet cyber attack. This may also be directly affected by the lack of certainty with the attribution applied to the nations. Regardless, Stuxnet provided a real world scenario for discussions about the impacts of speculative attribution on socio-political tension and cyber deterrence.

Conclusion

The Stuxnet cyber attack is the most high profile cyber attack to date. It was the product of some of the best programmers and control systems experts in the world. The operation resulted in the first ever known physical destruction of critical infrastructure assets via a cyber attack. This showed the world that cyber weapons can be as powerful as those in the traditional domains of warfare. In the end, Stuxnet offered a number of key takeaways and lessons learned for cyber decision makers.

The understanding that cyber attacks can be linked together for better operational success demonstrates synergy within the cyberspace domain. This takeaway empowers intelligence and cyberspace professionals to create better operational campaigns and defense strategies. The defense of cyber assets can be incredibly difficult. A cyber defender must protect the entire network whereas an attacker only has to find one successful attack vector. By monitoring cyber attacks and understanding their links, cyber defenders can better predict and counter the attacker's strategies.

The attack vectors, vulnerabilities, and strategies revealed in a cyber attack are openly available once the attack is discovered. In realizing this, cyber decision makers must attempt to think of all second and third orders of effect to an attack before initiating it. It is impossible to understand all impacts of a cyber attack before it is launched but by studying cyber events throughout history, including Stuxnet, a better understanding can be obtained. An attack that makes more friendly systems vulnerable than it destroys in an enemy will rarely be seen as a success. Stuxnet showed a number of vulnerabilities in Microsoft systems and control systems that can still be exploited but it was able to delay the Iranian nuclear program. However, by understanding cyber attacks, the vulnerabilities and strategies exploited can be used to increase

overall network defense. In the demonstration of cyberpower the strategies built can also act as a deterrent to future attacks.

Cyber deterrence requires a balance of understanding cyber capabilities and the risk that comes with using them. Stuxnet demonstrated that the risk of attribution would be one of the most perilous aspects of the operation. It also showed that regardless of the validity of the evidence found, all available clues will be used to apply speculative attribution. This shows attackers the benefit of leaving false evidence trails; it also shows defenders that they must be critical of every piece of evidence. For cyber decision makers the issues of attribution and cyber deterrence will always be two of the most worthwhile yet difficult aspects of cyberspace.

The cyberspace domain is complex and presents unique challenges. As the newest domain of warfare, it also has a lack of historical events and case studies that can be reviewed for lessons learned. Thus, it is imperative that the cyber events that have occurred be studied for all pertinent information that may be obtained from them. No better example of a successful cyber weapon currently exists than that of Stuxnet. In understanding this cyber attack and its takeaways, decision makers are better equipped to develop successful choices and strategies. In fully understanding demonstrations of cyberpower and the history behind them it is possible to decisively secure and win the cyberspace domain.