Can computer malware be used to inflict physical world consequences that change the way we view and interact with international geopolitics? As the world migrates closer and closer to a place that's entirely run by computers, this question may have more merit in recent years than it has in any other point in history. That question was catapulted into the general population's view when Stuxnet, one of the most infamous cyberattacks yet, was discovered in 2010. I chose this attack because I found the details surrounding the case interesting, along with the unsolved mystery surrounding it. This massive turning point in computer history sparked a conversation about how the next catastrophic 9/11-like event probably wouldn't require the physical hijacking of a plane, or the perpetrator even being in the physical presence of the people who will fall victim to it. So, what exactly happened because of Stuxnet? How was Stuxnet able to wreak as much havoc on the world as it did? How can we work to prevent the devastation that Stuxnet or similar cyberattacks may cause?

Stuxnet was an extremely sophisticated computer worm that targeted Iranian missile production. First, the worm runs reconnaissance and tries to determine what OS it's running on, as well as determine if any programmable logic controllers (PLCs) were connected to the machine. If none were found, Stuxnet would simply use the machine to replicate itself and spread to one that was connected to PLCs. Once it found a target PLC, the worm would attack the uranium refinement centrifuges to spin at high speeds. This caused the centrifuges to break down and halt the production of refined uranium. It would send messages to the PLC that said they were fully functional with no errors. The worm would then delete itself, making the problem incredibly difficult to detect and remediate until the centrifuge was completely destroyed. (Fruhlinger, 2017)

Due to its sophistication, it's believed that it could only have been developed by a nation-state hacker team as a weapon against the Iranian warheads. As far as we understand it, the worm is likely to have been developed in tandem by Israel and The United States, a claim which has been confirmed by security experts and U.S. officials. (Warrick & Nakashima, 2012) Stuxnet was unleashed on the Natanz

uranium refinement plant via a USB that contained the worm and was not intended to affect any other machine outside of that plant. The plant's network was supposedly sealed off from the internet but was somehow spread to an internet connected device. The contagious nature of the code caused it to spread to the rest of the world and is still around today, though it's effectively useless against most machines that have little to do with Uranium refinement. The US was under the impression that the code was modified by the Israeli government, which allowed it to spread past the agreed upon scope. (Fruhlinger, 2017) While Stuxnet was specifically developed to limit a containment breach, it proved that this technology could easily be developed to cause detriment to specific targets. Similar to a bioweapon, no computer malware is completely fool-proof to contain, despite how well its designed and how sophisticated it becomes. Many times, the sophistication is a leading cause in a virus or worm's ability to be unleashed onto the world with little to no control.

## Stars of the Stuxnet Disaster

As previously mentioned, Stuxnet was unleashed as a "defensive" countermeasure by the United States Government in cooperation with the Israeli Government, in an attempt to halt to the production of Iranian weapons. Some questions have yet to be answered about the motivations of these entities, as well as the response from the Iranian Government. To provide some background on this event, we must go more in depth about the history of the involved actors and detail any previous relations/actions that led to the launch of the attack.

First, let's focus on the attackers. The US government has been among key leaders in developing the modern attack vector of cyberwarfare. A good point in history to start from would be Executive Order 12333 signed by President Ronald Reagan on December 4, 1981. (Exec. Order No. 12333, 1981) This was an amendment to the National Security Act of 1947 that established new resources for the US government to collect intelligence. The order made it easier for US intelligence agencies to collect data

that the sitting president deems a threat to national security. While the order is packed with intel related statutes, it most notably created the Intelligence Community (IC) - a coalition of various intelligence departments with the power to execute intelligence collection orders. Meanwhile, in May of 2010, the National Security Association (NSA) created the United States Cyber Command (USCYBERCOM) years after its initial proposal in 2006. (United States Cyber Command, n.d.) The USCYBERCOM was tasked with preventing attacks against US assets and its allies, which makes it seem like a defensive committee. In reality, the USCYBERCOM appears to be more reliant on offensive attacks in the name of national security, as they have commonly used their cyberweapons to keep foreign entities – such as the Islamic State - in check. (Ryan, 2016) Either USCYBERCOM or the IC may be responsible for the Stuxnet attack, and until official documents regarding the attack have been declassified, we will not know which of these was sanctioned the attack. It's also entirely possible that these two agencies had nothing to do with the attack. However, I argue that these are the likely culprits given the nature of how they both operate and their goals for national security. Regardless, even with no official declassified document claiming responsibility, experts agree that the US and Israel are to blame for the initiative. In a leak attained via WikiLeaks, it was revealed that the US received advice from a German thinktank that halting Iran's missile production will provide a clear strategic value to the United States' defense efforts. (Halliday, 2011) The complexity of this worm, which required the power of a militarized national entity, added on top of the Iran/US tension at the time shows that the US had clear motive and means to carry out this attack. Something that no other country had, apart from its allies.

The United States and Iran have a long, complicated, and brutal history of conflict. From the 1979 Iranian Revolution through the Bush and Obama administrations, tensions between the two nations have increased dramatically. In 2002, President George Bush considered Iran an "Axis of evil.", a statement that enraged the Iranian government and some countries of Europe. (BBC, 2002) The US has

commonly denounced the actions of Iran and historically attempted to convince American citizens that Iran was public enemy number one. Due to this perceived evil, it wasn't difficult for the US government to justify their offensive attacks against Iran as a necessity for national and global security. This history is vital, because the peak of these tensions was around the mid to late 2000s, around the time Stuxnet was developed and deployed. During this era, the US received word that Iran was developing nuclear weapons that may be used to cause detrimental harm to enemy countries. Under the Bush administration, a plan of attack to halt production was devised, code-named Olympic Games. This plan included commencing development on a new piece of malware to accomplish the goals of Olympic Games, which later became known as Stuxnet. The plan was executed under the Obama Administration, near the very beginning of his term. (Sanger, 2012)

Now that the events leading up to the attack regarding the US and Iran are established, there are some questions about Israel's involvement. Why was Israel consulted for this attack and what benefit did they gain from aiding the US? Do they have the motive/means to alter the code to cause destruction as the US claims? Like the US, Israel has repeatedly denied claims of involvement in the Stuxnet worm and the evidence linking Israel to the attack is weaker than the evidence regarding the US, but there are still substantial claims that they also had the means and motive to carry out the attack. In 2010, around the time Stuxnet was discovered, Israel announced that they were officially adding cyberwarfare to their essential pillars of defense. According to Amos Yadlin, a major-general for the Israeli Defense Force (IDF), Israel is more than capable of executing cyberwarfare, and its forces are rigorously trained in the field. He claims that his country is able to be technologically independent due to its strong reputation in tech development. Most Israeli citizens are familiar with technological advances and provide valuable assets and skills to the IDF. (Williams, 2009) In Israel, young adults (18-26) are required by law to serve in the IDF, unless exempt. (Israeli Government , 1986) Because of this requirement, most members of the IDF are part of younger generations that have a firm grasp on

technology, due to the reliance on it during their upbringing. This makes the IDF a strong force to reckon with in the cyber world. Along with the US, Israel has also held a strong disdain towards Iran, citing antisemitism from its leaders. Iran has repeatedly made threats to dissolve the Jewish state and even funded multiple antisemitic terrorist groups that aimed to drive the Jewish people out of the country. (Nikou, 2021) There are quite a few easter eggs in the code of the program that hint at Israeli involvement, such as a piece of code that reads “19790509”. This could be a reference to the date the Iranian president, Mahmoud Ahmedinejad, spoke at Columbia University spouting antisemitism and denial of the holocaust. (Gross, 2011) Some suggest this may be a diversion thrown in to place the blame on Israel. Because Israel and the US have had a strong allyship for quite some time, it makes sense that they would team up to fight the common enemy of Iran. With Israel’s skills in cybersecurity and the US’s standing power, they were able to create a silent but destructive weapon that changed the means of warfare to require less blood spill than any other previous attack.

Finally, Iran’s reaction to the attack is an important aspect to consider when discussing the parties involved. Once discovered, Stuxnet had already infected over 30,000 IP addresses in Iran, so they assembled a team of highly skilled personnel to purge the worm from the systems. The state advised all plants to replace the controllers with non-Siemens PLCs, since the code seemed to be embedded into the systems and could evolve to attack again if safeguards are put in place. Replacing the controllers with the same manufacturer of PLCs could give the worm info to update itself, instead of eradicating itself. The worm was rapidly changing upon discovery, so the team needed to act fast and watch for any mutations. (Sobelman, 2010) Another Iranian plant – Bushehr – was affected as well, but according to Iran Daily (A state Run news outlet) the worm only affected personal computers and did not reach vital operational components. (Markoff, 2010) This hints at another reaction from Iran, disinformation. To conceal their plans, Iran tried to make the attack seem more dangerous than it was so the creators of the worm would assume they were successful in stopping the Iranian Nuclear program. However, a

study conducted by the Federation of American Scientists suggests that operational capacity of the program had increased in 2010 by 60% more than that of 2009. (Amarelo, 2011) The disinformation campaign was a smart move strategically, as Iran was able to create more weapons without raising suspicions from foreign countries. The campaign also worked to give Iran a few years of extra time to develop these weapons under the radar.

## Stuxnet Event Timeline: Stuxnet 0.5

While there's plenty left to be discovered about the origins of the Stuxnet worm, research from Symantec suggests that the party responsible for the worm began development as early as November of 2005, when the worm's Command and Control server was registered. This report details the existence of an early version of the worm that later became known as Stuxnet, called Stuxnet 0.5. The earliest record of implementation came to in November of 2007, when the worm appeared on a public malware scanning service. This primitive version worked slightly differently than how Stuxnet 1.x (the worm that was discovered in 2010) did. Stuxnet 0.5 was much less aggressive than its successor, though it's unclear exactly how much havoc this version caused to the Iranian Nuclear Program. Nonetheless, it's still important to discuss how Stuxnet 0.5 evolved into Stuxnet 1.x and what changes were made in the process. Fundamentally, the worm was developed based upon the Flamer platform, not the Tilded platform Stuxnet 1.x was based on. These different platforms of development indicate that this may have been a separate team that started the process than the team that finished the project. It also used different methods of replication. Stuxnet 0.5 spread only via infected Siemens Step 7 project files, which are stored locally on the target machine. Once a machine was infected, its Step 7 files are now compromised and ready to infect other machines. If a removable drive containing Step 7 files were connected to the machine after this point, those files would then become infected. This version was also spread via emails containing these Step 7 files, probably by employees that had no idea they were infected. This differs from Stuxnet 1.x, which uses both this method and exploits from Windows to help it spread. The two versions also differ in their attack goals. As previously stated, Stuxnet 1.x's main goal

was to control the speed of the uranium refinement centrifuges and cause them to spin faster than they were built for. Stuxnet 0.5 was focused on opening and shutting valves in the centrifuges to release gas that would destroy the equipment. It appears that this was easier to detect, so it makes sense that Stuxnet 1.x would change methods to reduce suspicion and increase the threat vector. Stuxnet 0.5 halted contact to the C&C server on January 11, 2009 and halted infecting new machines on July 4, 2009. Symantec has since recovered at least 4 different versions of the worm, but there may be many more out there. (McDonald, Murchu, Doherty, & Chien, 2013)

## Stuxnet Event Timeline: Stuxnet 1.001

The earliest iteration of a Tilded-based Stuxnet build found in the wild was compiled on June 22, 2009, according to the binary compiler timestamp. That's less than two weeks before v0.5 shut itself down. This implies that the v0.5 version showed promising results that warranted v1.001 to continue its work, with some glaring issues that needed to be omitted. Most notably absent, is the mechanism from 0.5 to control the valves of the system, as this process was replaced by controlling the speed of the centrifuges. (Robertson, 2013) v1.001 added 4 new exploits to the worm in addition to the previously mentioned Step 7 exploit: Print spooler RCE (CVE-2010-2729), Windows Server Service RPC RCE (CVE-2008-4250), WinCC default password (CVE-2010-2772), and NtUserRegisterClassExWow/NtUserMessageCall EOP (MS09-025). Interestingly, this version is the only version that uses a Microsoft reported vulnerability, probably because it was patched in a Windows update soon after discovery. (McDonald, Murchu, Doherty, & Chien, 2013)

The new additions to exploits of the worm allowed for the program to infect USB sticks that don't contain Step 7 files, increasing its threat footprint. It does this by exploiting the Windows Autorun feature so that the executable is run when the drive is plugged into an infected machine. It could also use the print-spooler exploit to spread throughout the network, as if it were a file being sent to a network printer. This is an obvious improvement from the previous iteration, which could only attack a small population of USB drives containing Step 7 files. On June 23, 2009 (the day after the binary

compiler's timestamp), program logs show the first company to be infected was Foolad Technic, a private engineering consultant in Iran. Almost a week later, another company called Behpajooh was infected with the worm. This location was chosen because of its ties to the Natanz plant, the enrichment facility that was the main target for the project. After Benpajooh was infected, the worm then moved to another company called Neda, chosen because it too was on a list of facilities involved in the enrichment of uranium. The Neda attack was flagged by an employee who posted that his department's PLCs were having issues with a Step 7 .DLL file after a USB is plugged into the machine, which were not present after a clean install. At this point in time, it's unclear how much time it took for the worm to reach Natanz, but experts put it around mid-July to August of 2009. This range is when the plant's centrifuge operations took a drastic dip compared to previous years. There is currently no tactile evidence that this decrease in operation was entirely due to the infection, but the binary compiler timestamps line up to support this theory. (Zetter, 2014)

Stuxnet Event Timeline: Stuxnet 1.100 and 1.101

The next known version of Stuxnet is v1.100, with a binary compiler timestamp of March 1, 2010. This iteration added 3 new exploits to the pile: Task scheduler EOP (CVE-2010-3888), LoadKeyboardLayout EOP (CVE-2010-2743), and Shortcut .lnk RCE (CVE-2010-2568). As noted above, this version did not use the MS09-025 exploit that v1.001 did. These additions allowed the worm to ditch the autorun mechanism and run based on the CVE-2010-2568 exploit, which uses the shortcut feature in Windows to execute the task scheduler for a more efficient infection strategy. Symantec also found another version in the wild, dubbed Stuxnet 1.101. this version was compiled on April 14, 2010, but there doesn't seem to be any major differences in either replication or exploitation from the previous version. (McDonald, Murchu, Doherty, & Chien, 2013)

## Stuxnet Event Timeline: The Aftermath

Every version of Stuxnet 1.x had code to stop running on June 24, 2012. This does not mean, however, that the Stuxnet framework and methodology was killed in the process. Upon discovery, the

Iranian president formed a committee to mitigate the Stuxnet disaster and recover any lost progress. It's unclear at this time how well they kept the destruction under control. As later revealed by U.S. officials, a similar attempt to halt nuclear weapons operations in North Korea was propagated by the U.S. but ultimately failed to accomplish its goal due to the tightly kept secrecy that North Korea holds dear. (Menn, 2015) In late 2010, another worm was discovered that was shockingly similar to how Stuxnet performed with a completely different purpose. This worm was found by Symantec, who named this succeeder Duqu. (Labratory of Cryptography and System Security, 2011) Later, in 2020, a fire broke out at the Natanz plant that Stuxnet originally attacked. According to Iranian officials, this was the result of a second version of Stuxnet initiated by Israel. This doesn't seem to have much evidence backing it up, however. The only evidence we have of this occurring is the accusation from the Iranian government, which may or may not be falsified to protect its national image. (O'Flaherty, 2020)

## Lessons Learned

The Stuxnet Attack has been vital to the conversations we hold regarding cybersecurity and using computer malware as a weapon of war. Mystery surrounding the attack is as ample as the damage it's done, and many are left with questions that may never receive answers. Where did it go wrong? Was Stuxnet created for doom from the start or was it simply meant to slow down weapon production as told in the US's story? These questions are valid, though it's doubtful that they will be declassified or clarified any time soon. Many details are still ambiguous regarding the attack, but that doesn't mean we can't learn anything from the details we do know. Here's how technical and social controls may have prevented this from happening, and how we can prevent another attack like this in the future.

Some might argue that the American government is doing the world a good deed by slowing the production of Iran's nuclear weapons through cyberwarfare tactics. After all, we're propagandized in our early lives to believe that our country is the greatest in the world, and that we pretty much only use our dominating military power for defense, not offensive attacks. While there may be some truth to this

statement, the US poked a sleeping bear just as it did when it developed the atom bomb to drop on Hiroshima and Nagasaki, killing over 200,000 people in the name of ending a war. The US claimed that developing this bomb would end the war and save lives. In reality, it ended up setting a precedent that allowed for other nations to follow their technology for large-scale attacks, which is how the Iranian Missile crisis came to be in the first place, leading to Stuxnet. This is the same problem with Stuxnet. While it's unlikely that a cyber-attack will kill hundreds of thousands, like the atom bomb did, Stuxnet was only a proof of concept that shows this can be an effective war vector. The issue is a deeply rooted systemic one, that the public is misinformed about the actions of the elites they elected to represent their thoughts and beliefs. The first step to preventing this from happening would be for the government to declassify credible information about its actions so that its citizens can decide if their government is making the right move. Representative democracy is an important part of how our country is built and we cannot make proper decisions on who makes up that representative democracy if the public is not informed. If the plans for Stuxnet were public, perhaps the open-source community could have seen how bad of an idea releasing a powerful computer worm into a foreign nation to commit an act of war was and voted accordingly.

Another social control that might help stop this from happening again would be for the UN to develop a modern version of the Geneva Convention document that clearly defines a violation of the terms of cyberwar. The Tallinn Manual was a study published in 2013, which showed that the United States did commit an act of force against Iran, which may violate international law. "Acts that kill or injure persons or destroy or damage objects are unambiguously uses of force", according to the manual. (Zetter, 2013) Unanimously, experts agreed that an act of force was committed. There was, however, some disagreement on whether or not the sabotage entailed an "armed attack", which would be a violation of the Geneva Convention's laws of war. (International Committee of the Red Cross, 1977) Under these laws, an armed attack is classified as provoking international hostilities. If the US were

found guilty of violating these international laws, Iran would have the legal right to use force in self-defense, thus fueling another unnecessary war. Because the current international legislature has not accounted for cyber-attacks, there is some legal grey area that should be clarified.

On top of the social controls that would address the systemic issues of the United States' actions, Iran is not blameless in their vulnerability and contingency planning. While the social controls would clearly aid in combatting human nature, technical controls could have also played a defensive part that may have protected Iran from devastation if implemented at the time. For instance, Iran could have properly managed encrypted keys so that the worm would never have the chance to find information. (Kleinerman, 2012) Due to the nature of the worm, information gathering is paramount to ensure a successful attack. Stuxnet must run checks to find the PLCs and will not do anything if these PLCs are not connected to centrifuges. If that information were properly encrypted over the internal network using a method like AES, Stuxnet would have a hard time performing reconnaissance on that network. This would drastically slow its spread and minimize the damage done to the Natanz plant. It seems odd that this wasn't thought of by the higher-ups in the operation, but hindsight is 20/20 and they had no reason to believe that this facility would be targeted, considering how well they thought they concealed the information surrounding the plant. Companies can learn from this mistake and plan accordingly by setting up a proper key management system that would make it much more difficult for an unauthorized party to access encrypted data. While a private company cannot be held to the same standards as a federally funded uranium plant, the principles still apply and should be considered for a company storing any sensitive data, no matter how small that company is. Proper encryption should be a top priority for Cybersecurity experts tasked with designing the network security policies of the organization.

Finally, this attack could have been prevented if the Natanz plant use policy prevented external USB drives from connecting to PLCs, since that was initially how it got into the plant in the first place.

Policies such as this should be written in a way that would either prevent employees from using them entirely, or keeping a log of every single USB that's plugged in. Every Windows machine stores these entries in the Registry to reference later, and this can be recovered through digital forensics and scripting intended to prevent new sticks from connecting. In fact, there is a hack that occurs in the USA television show, Mr. Robot, that takes advantage of a person's ignorance on what danger DVD/CD drives can be, and the same principle applies to USB drives. In this episode, a street musician hands out CDs asking for people to listen to his music. What these patrons didn't know is that the CD contained an exe that allowed the musician to take complete control over the user's computer and access the webcam without them knowing. This is relevant, because it shows that we should be cautious about all unfamiliar devices on our network and desktops. In the US, the Department of Defense released guidelines to help combat external USB drive usage throughout their vendors' organization. In section 3.1.20, the document explicitly states, "Limit use of organization portable storage devices on external systems." (Ross, Pillitteri, Dempsey, Riddle, & Guissanie, 2020) This prevents exfiltration of classified data, and the document provides a specific policy that can be violated and handled accordingly. If there were no written security policy on this, it would be difficult to prosecute someone for using a USB stick. The same guidelines would apply for external sticks on internal network, opposition of which can lead to another Stuxnet. Stuxnet was a ruthless weapon designed to take the tides of cyber-warfare to unchartered territories for the first time in history. Though, through proper education and the controls listed above, we can aim to prevent this attack vector from being capable of irreparable mass destruction.

# Bibliography


Amarelo, M. (2011, January 21). *Federation of American Scientists*. Retrieved from New FAS Report Demonstrates Iran Improved Enrichment in 2010: https://fas.org/press/news/2011/issuebrief_iran.html

BBC. (2002, February 11). *Analysis: Iran and the 'Axis of Evil'*. Retrieved from BBC: http://news.bbc.co.uk/1/hi/world/middle_east/1814659.stm

Fruhlinger, J. (2017, August 22). *What is Stuxnet, who created it and how does it work?* Retrieved from CSO Online: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Gross, M. J. (2011, March 2). *A Declaration of Cyber-War*. Retrieved from Vanity Fair: https://www.vanityfair.com/news/2011/03/stuxnet-201104

Halliday, J. (2011, January 18). *WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank*. Retrieved from The Guardian: https://www.theguardian.com/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear

International Committee of the Red Cross. (1977, June 8). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts.* Retrieved from International Committee of the Red Cross Database: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079

Israeli Government . (1986, January 30). *Defence Service Law 5746.* Retrieved from Israel Ministry of Foreign Affairs: https://www.mfa.gov.il/mfa/mfa-archive/1980-1989/pages/defence%20service%20law%20-consolidated%20version--%205746-1.aspx

Kleinerman, A. (2012, March 22). *Could Encryption Have Stopped Stuxnet.* Retrieved from Townsend Security Data Privacy Blog: https://info.townsendsecurity.com/bid/54381/Could-Encryption-Have-Stopped-Stuxnet

Labratory of Cryptography and System Security. (2011, October 14). *Duqu: A Stuxnet-like malware found in the wild*. Retrieved from crysys.hu: https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

Markoff, J. (2010, September 26). *A Silent Attack, but Not a Subtle One*. Retrieved from The New York Times: https://www.nytimes.com/2010/09/27/technology/27virus.html

McDonald, G., Murchu, L., Doherty, S., & Chien, E. (2013). *Stuxnet 0.5: The Missing Link.* Mountain View, CA: Symantec.

Menn, J. (2015, 29 May). *Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed*. Retrieved from Reuters: https://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529

Nikou, S. N. (2021, Auguat 10). *Timeline of Iran's Foreign Relations*. Retrieved from United States Institiute of Peace: https://iranprimer.usip.org/resource/timeline-irans-foreign-relations

O'Flaherty, K. (2020, July 4). *Stuxnet 2? Iran Hints Nuclear Site Explosion Could Be A Cyberattack*. Retrieved from Forbes:

https://www.forbes.com/sites/kateoflahertyuk/2020/07/04/stuxnet-2-iran-hints-nuclear-site-explosion-could-be-a-cyberattack/?sh=c5be5f525ad2

Robertson, A. (2013, February 26). *Newly discovered Stuxnet variant sheds light on the virus' development*. Retrieved from The Verge: https://www.theverge.com/2013/2/26/4032680/newly-discovered-stuxnet-variant-sheds-light-on-virus-development

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020, February). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* Retrieved from www.Nist.gov: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Ryan, M. (2016, July 15). *U.S. military has launched a new digital war against the Islamic State*. Retrieved from Washington Post: https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html

Sanger, D. E. (2012, June 1). *Obama Order Sped up Wave of Cyberattacks Against Iran*. Retrieved from The New York Times: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Sobelman, B. (2010, September 27). *IRAN: Speculation on Israeli Involvement in Computer Malware Attack*. Retrieved from Los Angeles Times: https://latimesblogs.latimes.com/babylonbeyond/2010/09/israel-questions-about-the-stuxnet-attack-on-iranian-computers.html

United States Cyber Command. (n.d.). *Our History*. Retrieved from cybercom.mil: https://www.cybercom.mil/About/History/

Warrick, J., & Nakashima, E. (2012, June 2). *Stuxnet was work of U.S. and Israeli experts, officials say*. Retrieved from The Washington Post: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.3283038083d7

Williams, D. (2009, December 15). *Spymaster Sees Israel as Cyberwar Leader*. Retrieved from Reuters: https://www.reuters.com/article/idUSTRE5BE30920091215

Zetter, K. (2013, 25 3). *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'*. Retrieved from www.wired.com: https://www.wired.com/2013/03/stuxnet-act-of-force/

Zetter, K. (2014, November 3). *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Retrieved from Wired: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/