2019

Cyber warfare in the 21st Century

And its effect on Public Infrastructure and its Cyber security

Hasan Mohammad Jared Borah

Abstract

With the digital world expanding as technology continues to advance the growth of malicious software and those with the skills and willingness to use it has increased exponentially. Where some have celebrated this new interconnectedness, others have identified potential pitfalls. The age of the Internet of things is creating a more complex cyberspace filled with threats. Cyber Warfare is becoming more prominent in the 21st century. With the United States, Russia and Iran expanding their knowledge, it is important to examine the policies of these countries, their operational forces, and analyze the attacks these countries have done. This is the primary way to determine how this will affect future standards of information security and the strategies public infrastructure must take. The electrical grid, gas pipelines, nuclear power plants, water supply, sewage treatment, public transportation system and internet infrastructure are what we define as public infrastructure. As an increasing number of nation states have developed cyber warfare capabilities, the threat to public infrastructure in United States increases every year. The industry and its partners should begin developing all-inclusive cybersecurity strategies. Adopting a set of security standards, sharing information regarding vulnerabilities/attacks and best practices is the only way forward. As we open more frontiers with advancements in artificial intelligence, there will always be those who wish to exploit them. Thus, a static mindset in security must be discarded permanently if we are to design novel security solutions to ever changing world

Introduction

The use of malicious software such as viruses or worms has become increasingly common in society today. In 1988, the Morris worm was one of the first computer worms to spread across the internet. This worm was written by Cornell graduate Robert Morris and released from M.I.T on November 2, 1988. Once this worm was released, it affected over six thousand computers within 24 hours that were connected to the internet. It took over two days to purge the worm from the affected computer systems. This event became a starting point to a whole generation of new hackers, and digital assaults continue to affect computer systems around the world today.

With the digital world expanding as technology continues to advance the growth of malicious software and those with the skills and willingness to use it has increased exponentially. As we enter the age of "The Internet of Things" computers have taken new forms ranging from kitchen appliances to the car in your garage. Where some have celebrated this new interconnectedness, others have identified potential pitfalls. In recognition of the growing threats and potential usefulness this poses, Nation-states have begun to develop their own offensive and defensive capabilities. From Great powers such as USA, China, and Russia to smaller powers such as North Korea and Iran. Offensive cyber actions by state actors have already been documented in Estonia (2007), Georgia (2008), Iran (2008), Sony (2014), and Ukraine (2017). .

Technology advancements are expanding the frontiers of society. The age of the Internet of things is creating a more complex cyberspace filled with threats. Cyber Warfare is becoming more prominent in the 21st century. With the United States, Russia and Iran expanding their knowledge, it is important to examine the policies of these countries, their operational forces, and analyze the attacks these countries have done. This is the primary way to determine how this

will affect future standards of information security and the strategies public infrastructure must take.

United States

Beginning with the United States, the first law of vital importance is the 2016 National Defense Authorization Act (NDAA). This policy elevated the United States Cyber Command (USCYBERCOM) into a unified combatant command under President Obama. The law also included a budget to supply a more direct means of funding for the research and the purchase and use new software and technologies in the United States. The law first vetoed by President Obama in October of 2015 until he finally signed a modified version in November of the same year. In the Trump era, a new law would augment the NDAA act. Known as the Cybersecurity and Infrastructure Security Agency Act of 2018, signed into law by Donald Trump in November of 2018. The act created a new agency, the Cybersecurity Infrastructure Security Agency (CISA) and gave it mandate to identify Untied States entities that could be at risk of an incident, assess risks of their vulnerabilities, supply guidance and federal resources and capabilities to better counter cyber security risks. Together with National Protection Programs Directorate (NPPD) and CISA work to provide a centralized and coordinated policy to protect both public and private institutions from both external and internal cyber threats. It also allows the federal government to supply cybersecurity tools to better combat any future issues that are sure to rise in the Cyberspace infrastructure. The requested budget for Cyberwarfare defense infrastructure in the fiscal year of 2019 amounted to 14.98 billion dollars. The Defense Department is earmarked to receive over 57% of the budget, which includes funding military capabilities to conduct cyber warfare attacks against potential adversaries that could pose as threats to the United States. Cyberspace. This is meant to act as a deterrent to any potential external actors, both foe and ally

alike. The department of Homeland Security was allotted 12% of the funding as the Department of Homeland Security is the leading federal agency of securing information technology systems that belong to the federal government.

Shifting from policy to operational units. the United States has recently created a unified cyber command in a bid to centralize the cyber forces from the many branches of the United States Military. The USCYBERCOM has 5 service components from 4 branches of the Military. This 133-team, 6,200-person cyber mission force is now fully operational. (US Army 2019) This Cyber Force is focusing on real-world cyberspace that has become a new war front around the world. Some of the threats that have been the focus for USCYBERCOM are ISIS, peer adversaries, and many other global cyber threats. One of the many components of this new command that has made substantial progress in the employment of cyber tactics is the United States Army Cyber Command. Their mission is maintaining security in the cyberspace and conducting electronic warfare. They handle monitoring of a myriad of cyber threats, improving their cyber operations, developing and recruiting of cyberspace professionals in the Army. The U.S. Army Cyber Command conducts operations around the world 24 hours and 7 days a week. With over 16,500 soldiers and civilians that work across 4 states and 5 cyber centers all around the world. (US Army 2019) These states include Virginia, Maryland, Arizona, and Georgia.

With the Policies and brief overview into the operational units of the United States examined, we move to an analysis of the attacks attributed to the United States. The attack on Iranian nuclear centrifuges via Stuxnet worm. The malware development of Stuxnet was one the most expensive and complex ever made. (Kushner 2014) It was first uncovered in 2010 but is believed to have been in development since 2005. Given the code name “Operation Olympic Games, Stuxnet is multi-layered attack specifically targets three different systems. First, it attacks the Windows

operating system via four zero-day attacks. Second, it then infects the Siemens Process Control system PCS 7, the WinCC SCADA system and STEP7 industrial software applications that run on the Windows operating system. Lastly, it attacks one or more Siemens S7 programmable logic controllers (PLCs) used by Iran. (Broad, Markoff, & Sanger, 2011) It specifically attacks those PLC systems with frequency drives from the vendors Vacon and Fararo Paya. (Chien 2010) The PLCs automates industrial machinery processes including centrifuges for separating nuclear material. Stuxnet also did intelligence work, collecting information on industrial systems. The design of the malware intended was solely for Iranian Nuclear program. Intended to cause as little to no collateral damage. Stuxnet eventually did end up on the internet but caused minimum damage. When the worm infects a computer, it checks if it is connected to a programmable logic controller (PLC) which is how a computer interacts and controls with the automated nuclear centrifuges being used in Iran. Once the worm infects the PLC, it alters the programming of it which leads to the centrifuges spinning at a rate fast enough to cause severe damage to the centrifuges. PLCs are also designed to monitor the centrifuges alerting users of normal activities, errors occurring or damage. To counteract the PLC, the malware used man-in-the-middle attacks to report to monitoring computer users that no errors were occurring, and operations of the centrifuge systems were normal until it was too late to correct. The purpose of this was the US and Israel governments wanted to prevent Iran from developing any nuclear weapons that could be used against them. Both the US, and Israel have seen this as a nonviolent alternative from trying to use weapons against Iran.

The next attributed attack conducted by the US is the program PRISM. PRISM is an acronym which stands for Planning Tool for Resource Integration, Synchronization, and Management. (Murse 2019) Also, known as SIGAD US-984XN, the program brought to light by Edward

Snowden an NSA contractor, who is one of the most famous Whistleblowers in the 21st century. The program, launched by President Bush's Presidency, given legal authority by the Protect America Act in 2007 and operated by the National Security Agency (NSA). Their reasoning behind the launch of PRISM was to collect and analyze sensitive data that was privately stored and operated by major web companies. The Protect America Act allows the attorney general, and the director of national intelligence to inform in a classified document the methods the US would use to collect intelligence on foreigners overseas each year but did not require any specification of the targets or their location. Once approval of the secret order by a FISA court judge, the NSA could compel USA companies like Google to send content/metadata to NSA. The content included video and voice chat, voice-over-IP chats, videos, emails photos, file transfers, and social networking. (Greenwald & MacAskill, 2013). The metadata included phone records that reveal the participants, times, and durations of calls. Supposed safeguards were in place if more than 51% of the content involved a US citizen not involved with "terrorist activities." Coupled with the NSA having the ability to pull data directly from undersea telecommunication's cables information, it gained unprecedented amounts intelligence on citizens, allies, and foes alike. (Sottek, 2013) This allowed NSA analysts to search and listen to the communications of US Citizens and others without court approval and supervision. (Greenwald 2013). The NSA excused this by saying it was necessary to protect the US from potential terrorist attacks, and even preempt hostile cyber activities. The program was successful in preventing a terrorist operation in 2009 when an Islamist militant was planning to bomb the New York subway system. Fortunately, the police were notified and able to prevent this attack from happening. It was so effective that then president Obama defended the program as he

believed that it is important to understand that it is impossible to have 100 percent security with 100 percent privacy.

Russia

The Russian government believes it is in an existential struggle with foes both internal and external seeking to challenge it in the cyberspace. The internet, and its free flow of information, is viewed as both a threat and an opportunity. (Connell, M., & Vogler, S. 2016) Many within the Russian government perceives the struggle within cyberspace to be constant and ongoing. The Russian government does not use the term cyber warfare but prefers to view cyber warfare as a facet within the broader category of information warfare. A concept that includes anything from propaganda, psychological operations, network operations and electronic warfare. History has shown that the Kremlin has a relativity low abhorrence in utilizing the cyber operations in an offensive nature. A central belief of Russian military brass is the that one of the features of modern military conflict is "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force" (Russia Federation 2010). In the previous decades the Russian military has been slow to incorporate cyber warfare for myriad of financial and structural reasons. Once of which was the view that cyberwarfare was within the of realm its intelligence community. The Federal security service (FSB), the KGB's successor has vigorously attempted to prevent the military from entering this field as it views it within its realm of influence. Since Putin has come to power, the Kremlin has bolstered the military's offensive and defensive cyber capabilities of its armed forces. According Russian public records it is spending on military cyber capabilities is 70 million USD per fiscal year. (krymrossiyskaya 2013) The actual amount is believed to be much higher. Russia's cyber forces are currently based around the Ministry of Defense. Ministry of defense has been able to create

new units that include jobs like hacking into fighter jets and blinding their flight paths. The development of hacking skills and planting malicious software has been a major priority. The units that are being formed are known as information troops. The information troop is based around the use of programmers, mathematicians, cryptographers, and others. (Connell 2016) This expansion has made it easier for Russia to recruit new members for offensive, and defensive attacks that were to occur in their cyberspace. One example of this is their S-400 missile defense system which is said to have cyber defense capabilities. Cryptographers have made it difficult for many external threats to try to gain access onto their classified military networks. Cyber-criminal syndicates have increasingly become a mainstay in Russian offensive cyber operations, due to the effective deniability they provide and the ease with which they can be mobilized. This crowd-sourcing approach that has defined how the Kremlin conducted its operations in the past is likely to be replaced by more focused approaches, with the FSB and other agencies playing a more dominate role. (Connell 2016).

Two attacks that were carried out by the Russians that worthy of note were the DNC hack in 2016 and the 2008 Ossetia War Cyberattack. The DNC hack was an attack that would end up costing Hillary Clintons in the Election due to the Russians gaining access into the Democratic National Committee (DNC). This all began back in March of 2016. Spear-phishing emails were sent to all members of the Clinton campaign. John Podesta clicked on one of these emails and was asked to enter his password. This allowed the hackers to gain access into his account, and in the Democratic Congressional Campaign Committee (DDDC) server. They stole the credentials of a DDDC worker that had access to the DNC server, and thus were able infiltrate the DNC. For the next two months between April, and June; the Russian military agency called GRU was able to compromise over 30 computers that were connected to the DNC server. Each computer being

infected with malware. By July of 2016, Wikileaks release more than 20,000 emails, and documents from the DNC server. This all happens three days before the Democratic National Convention. In August of that year, one of the members of Guccifer 2.0 (a hacker group with known ties to the Russian government) contacted Donald Trump and asks him what he thinks of the documents being released. These emails included personal information about the Clintons presidential campaign, other members of her campaign, and other sensitive information. All of this happened because Podesta clicked on an email that he should not have opened. This would end up costing Hillary Clinton from becoming president, and lead to Donald Trump winning the Presidential election to become the 45th President of the United States.

The second attack that was carried out by Russia was the Ossetia War cyber-attack back in 2008. This cyber-attack Russia used against the country Georgia would cause their cyber infrastructure to crumple. Russia cyber operations began weeks before both countries went into battle. The Russia attacks at first were psychological in nature as when the Georgian Presidents website was hit by DDoS attack. They even portrayed Georgia President Mikheil Saakashvili as Hitler in a slideshow presentation. Georgia websites were being defaced by the Russian hackers as tensions were continuing to build. This would eventually lead to a 5-day battle between Russia and Georgia that took place in the South Ossetia. On the first day the war began, Russian backed hacktivist websites, provided lists of Georgian sites to attack, with instructions and downloadable malware. (Connell 2016). As Russian forces drove south into Ossetia region, an onslaught of DDoS attacks took aim at Georgia's information infrastructure, disrupting government communications and the defacing of government websites. Even civilian entities were not spared. Georgian banks, commercial transportation, and private telecommunications were

successful attacked bring civilian life to a temporary standstill. This attack was widely seen as the first instance of a wide scale cyber operation in conjunction with military operations.

.

Iran

Iran is working to develop, support, and operate cyber warfare capabilities ever since the Ayatollah Khamenei created the Supreme Cyber Council on March 2012. In his speech, he pointed out the risks and opportunities inherent in cyberspace. The council's current mission is instituting high-level policy within the realm of security. The nation has developed an extensive network of academic research institutions dealing with information technology, computer and electronic engineering, and math. To this end, Iran has spent over billion dollars. (Siboni 2012) Iran seeks two defensive goals. The first is external and revolves around the idea of encapsulating or enveloping its critical infrastructure and information systems from cyber-attack. A lesson learned the hard way after Stuxnet virus severely damaged Iranian centrifuges. The second goal is internal nature with an emphasis being to prevent the internal opposition for whom cyber space is key in organizing anti-regime activities, the distribution of information and communication. One of the central organizations is the Cyber Defense Command, which functions under Iran's Passive Defensive Organization. This cyberspace organization includes representatives of the ministries of communications, defense, intelligence, and industry, and its mission is to develop a defensive doctrine against cyber threats. Another cyberspace body whose mission is defensive is the Information Security Center, under the purview of the communications and information technology ministry. The center runs rapid response teams for emergencies and cyber-attacks. Iran has also created the Committee for Identifying Unauthorized Sites, which supervise Iranian internet usage, with emphasis on internet cafes which allow

anonymous web surfing. (Bastani 2016) To carry out this goal further, the Iranian have begun creating the own independent communications network and a nationwide intranet. On the offensive front Iranians see cyber warfare as central tenets of its military doctrine of asymmetrical warfare. Cyber warfare gives Iran the ability to severe damage on an enemy superior in technological and military capabilities. The Revolutionary Guards have made Iran a leading nation in the realm of cyberspace warfare, with capabilities including the ability to install malicious code in counterfeit computer software, mechanisms to control servers, the disabling of communications networks, the development of novel computer viruses, tools for penetrating computers to gather intelligence, and delayed action programs. Taking a page out of their Russian allies, there are increasing links between the Revolutionary Guards and hacktivist groups in Iran and in former Soviet states that are willing to operate against their perceived enemies at home and around the world. This increase use of outsourcing allows Iran to maintain distance and deniability about Iran's involvement in cyberspace warfare. A well-known hacker group with links to the Iranian government is the Ashiyane (meaning nest in Farsi) Digital Security Team. These revolutionary partisans motivated in supporting the Iranian Clerical regime and its Islamic Revolution ideology. They have been known to target the enemies of the regime for attack. (Insikt Group, 2019) The attacks have ranged from the benign, such as website defacement to highly destructive attacks, such as the 2012 attack on Saudi Aramco that wiped over 30,000 computers.

Now that we have a better picture into the current state of Iranian Cyber capabilities, will shift to analysis of Iranian attributed attacks. In March 31st of 2015, Turkey's power grid was maliciously attacked. 44 out of 81 provinces, roughly half of Turkey's provinces and over 40 million people were affected by this attack. The massive power outage lasted for 12 hours

affecting everything from airports, the transportation system, hospitals, elevators, water supply and sewage. The attack was likely a result of a thumb drive attached to a computer system that was connected to electric grid systems. The malicious code could respond to commands remotely and was activated by an unopened email message. The attack targeted Turkey's power distribution network and not is better protected central power grid. Giving it the ability to turn on and off power at will. The attackers turned the power back on once they felt Turkey had learnt its lesson. (Halpern 2015). The Triton Attack was detected in June 2017 in a petrochemical plant in Saudi Arabia. At first the hackers managed to gain access to the unnamed petrochemical company's corporate IT network. From the IT network they proceeded to gain access to one of its chemical plant's networks through poorly configured firewall and from there into an engineer's workstation form either exploiting an unpatched flaw in the windows code or through social engineering of employee to gain their credentials. (Giles 2019) Because the workstation communicated with the plant's safety instrumented systems, the attackers were able to learn the model of the systems' hardware controllers and its firmware. This allowed the hackers to mimic the protocol and discover a zero-day vulnerability. The vulnerability allowed them inject code into the safety systems' memories that ensured they could access the controllers whenever they wanted. Once this was achieved the intruders could have ordered the safety systems to disable themselves and then using other malware cause a disaster to ensue. Only a flaw in malicious code caused the safety system to shut down prematurely and allowed investigating technicians an opportunity to discover the attack. (Johnson 2017)

Public Infrastructure

Shifting our focus onto public infrastructure and how best to develop successful cyber defensive strategies, we must first define what we consider public infrastructure. The electrical grid, gas

pipelines, nuclear power plants, water supply, sewage treatment, public transportation system and internet infrastructure are what we define as public infrastructure. As an increasing number of nation states have developed cyber warfare capabilities, the threat to public infrastructure in United States increases every year. As seen in figure 1 the number of reported cyber incidents have gone up on an almost yearly basis since 2010.

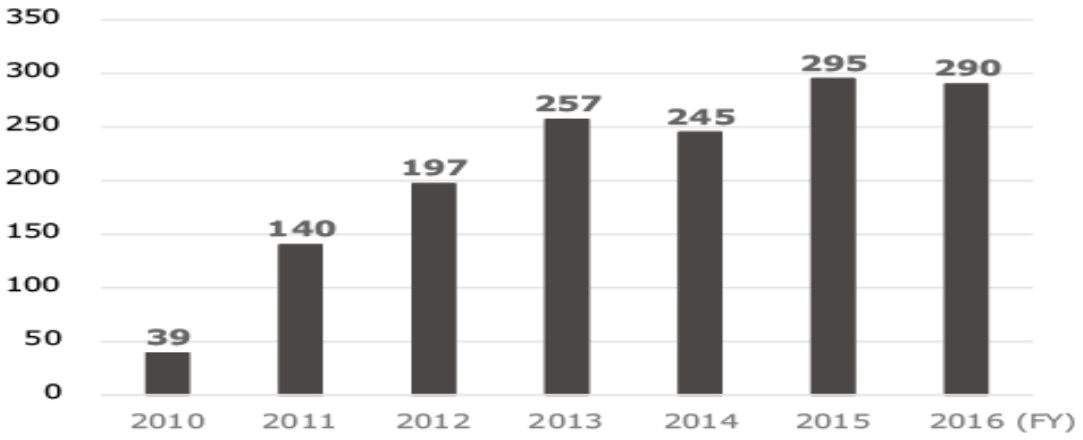

Figure 1 Number of incidents handled by U.S. ICS-CERT. NOGUCHI, M., & UEDA, H. (2017). Number of incidents handled by U.S. ICS-CERT. In an Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures. Retrieved June 24, 2019, from htttps:// www.nec.com/en/global/techrep/journal/g17/n02/170204.html

The methods used in most cyber incidents against public infrastructure are as follows; Social Engineering, Malware, DDoS, and Sabotage attacks. To reduce the likelihood and success of an attack an industry wide strategy must be put in place. From a regulatory perspective, there needs to be an increase regulation requiring developers and manufacturers of IoT products to have security functions and capabilities. Most PC security solutions cannot even run on embedded devices and manufacturers have no incentive to create them as it would drive up development costs. The most critical systems that require security solutions are the supervisory control and data acquisition (SCADA) systems that gather real-time measurements from subunits and send out control signals to equipment, such as circuit breakers. Increasing the liabilities and the fines manufacturers would face, creates incentive for the industry to change. The industry and its

partners should be developing all-inclusive cybersecurity strategies. Adopting a set of security standards, sharing information regarding vulnerabilities/attacks and best practices is the only way forward. On a Managerial front, increases in education for all employees regarding internet practices will help employees avoid the many social engineering pitfalls that exist in the cyber realm. Increases in training for all critical employees are necessary so they can increase their skills in threat awareness and attack recognition. On the technical front, distribution networks need to have a more sophisticated and well-rounded security systems in place. As seen with the incident on Turkey's electrical grid, distribution networks are often overlooked. The development of industry specific VPNs, Firewall, and IDPSs will not only better protect systems from attack but will aid in developing standards. Another solution is the creation of nationwide intranet for public utilities, this would limit the pool of potential attack vectors and better secure the nation from external threats. Instituting a dual system control is expensive cost but is necessary in mitigating the eventuality of a successful attack. Public utility commissions and the federal government should help utilities recover the costs of running two systems. The federal and state governments should also begin to invest in strategies to protect infrastructure from cyberattacks on a state and local level. By doing so the nation can create a multi-layered defense that would act as a deterrent in of itself.

Conclusion

We must first acknowledge the limitations in knowledge regarding the current capabilities of the leading cyber capable nations. The most advance capabilities and technologies remain classified and will only become known once they are used. Another fact that must be mentioned is with any security system, there is no guarantees that any system will be prevent all threats. False positives whether intentional or otherwise create difficulties for any security system and create a

laxness in attitude with the users. It is only with vigilance and dynamic behavior can a defense be viable. As we open more frontiers with advancements in artificial intelligence, there will always be those who wish to exploit them. Thus, a static mindset in security must be discarded permanently if we are design novel security solutions to ever changing world.

References

Tax Payers for Common Sense. (2019, January 18). Federal Funding for Cybersecurity. Retrieved June 23, 2019, from https://www.taxpayer.net/national-security/federal-funding-cybersecurity/

Greenwald, G., & MacAskill, E. (2013, June 07). NSA Prism program taps in to user data of Apple, Google and others. Retrieved June 21, 2019, from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

H.R. 1735 (114th): National Defense Authorization Act for Fiscal Year 2016. (2015, October14). Retrieved June 20, 2019, from http://www.govtrack.us/congress/bills/114/hr1735/summary

Rathnam, L. (2017, April 19). PRISM, Snowden and Government Surveillance: 6 Things You Need To Know. Retrieved June 23, 2019, from https://www.cloudwards.net/prism-snowden-and-government-surveillance/

Sottek, T. (2013, July 17). Everything you need to know about PRISM. Retrieved June 29, 2019, from https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

Fruhlinger, J. (2017, August 22). What is Stuxnet, who created it and how does it work? Retrieved June 21, 2019, from https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

Chien, E. (2010, November 12). Stuxnet: A Breakthrough. Retrieved June 23, 2019, from https://www.symantec.com/connect/blogs/stuxnet-breakthrough

Kushner, D. (2013, February 26). The Real Story of Stuxnet. Retrieved June 22, 2019, from https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Pomerleau, M. (2018, May 18). Cyber Command reaches critical staffing milestone. Retrieved June 23, 2019, from https://www.fifthdomain.com/dod/cybercom/2018/05/17/cyber-commands-cyber-warriors-hit-key-milestone/

US Army. (2019, April 4). About Us. Retrieved June 23, 2019, from https://www.arcyber.army.mil/Organization/About-Army-Cyber/

About Army Cyber Command. (n.d.). Retrieved from https://www.goarmy.com/army-cyber/about-army-cyber-command.html

Murse, T. (2019, March 27). What Does the NSA Acronym PRISM Stand For? Retrieved from https://www.thoughtco.com/nsa-acronym-prism-3367711

The Military Doctrine of the Russian Federation, approved by Russian Federation presidential edict on February 5, 2010 (translated). Accessed at http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

Connell, M., & Vogler, S. (2016). Russia's Approach to Cyber Warfare (pp. 7, Tech.). Arlington, VA: Center for Naval Analyses..

(2013). Retrieved June 23, 2019, from http://day.kyiv.ua/ru/article/ekonomika/krym-rossiyskaya-kiberstrategiya-voyny

The Russian Military Creates Its Own Cyber Troops. (2015, May 28). Retrieved from https://warisboring.com/the-russian-military-creates-its-own-cyber-troops/

Person. (2019, April 18). Russians Hack the DNC's Server: A Timeline. Retrieved from https://www.wusa9.com/article/news/politics/mueller-report/russians-hack-the-dncs-server-a-timeline/65-bd1326a7-7ed5-4cd7-92a3-63eed75f1bd9

Broad, W. J., Markoff, J., & Sanger, D. E. (2011, January 15). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. Retrieved June 26, 2019, from https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all

Danchev, D. (2008, August 12). Coordinated Russia vs Georgia cyber attack in progress. Retrieved from https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/

Harris, C. (2018, August 07). Europe's forgotten war: The Georgia-Russia conflict explained a decade on. Retrieved from https://www.euronews.com/2018/08/07/europe-s-forgotten-war-the-georgia-russia-conflict-explained-a-decade-on

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017, February 01). Protecting drinking water utilities from cyberthreats. Retrieved June 23, 2019, from https://www.osti.gov/pages/servlets/purl/1372266

Siboni, G. (2012, October 15). Iran's Cyber Warfare. Retrieved June 23, 2019, from https://www.inss.org.il/publication/irans-cyber-warfare/

Bastani, H. (2016, February 06). Structure of Iran's Cyber Warfare. Retrieved June 24, 2019, from http://www.strato-analyse.org/fr/spip.php?article223#outil_sommaire_3

Insikt Group. (2019, January 16). The History of Ashiyane: Iran's First Security Forum. Retrieved June 20, 2019, from https://www.recordedfuture.com/ashiyane-forum-history/

Halpern, M. (2015, April 22). Iran Flexes Its Power by Transporting Turkey to the Stone Age. Retrieved June 23, 2019, from https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/

Giles, M. (2019, March 06). Triton is the world's most murderous malware, and it's spreading. Retrieved June 23, 2019, from https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/

Johnson, B. (2017, December 14). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure « Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure.

Retrieved June 22, 2019, from https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html