5-2021

When Does a Cyber Crime Become an Act of Cyber Warfare

Luke Dickeson
ldickeson@unomaha.edu

When Does a Cyber Crime Become an Act of Cyber Warfare?

by

Luke Dickeson

Honors Thesis

University of Nebraska-Omaha

4/27/2021

Introduction and Importance

Since the existence of the online world, cyber attacks have been a threat. As the online world has developed and evolved so have the attacks on them. The advancement of technology has meant the advancement and increased complexity of cyber attacks.

Cyber attacks can be broken into two categories. The first is cyber crimes, and the second is cyber warfare. The difference between these two is not black and white, but rather a very murky grey. There is no agreed upon definitive line that separates cyber attacks and cyber crimes. This is because the definitions are so eerily similar, and there is not any agreement within the legal realm for when a cyber crime becomes an act of cyber warfare. While it is easy to identify a cyber crime, it is significantly harder to identify when that cyber crime becomes cyber warfare. The question that must be answered is at what point does a cyber crime become cyber warfare.

The laws of countries and international organizations have been notoriously slow when it comes to keeping up with fast-paced technology. Countries and international organizations that have laws that address the cyber realm have similarities, but they also have stark differences. These differences make it harder to define both cyber crimes and cyber warfare, as well as the line between the two. If this line can be defined, then the world can unite in the fight against cyber crimes and cyber warfare. Until it is defined, then it will continue to be a grey area in the cyber realm, and the legal realm.

Cyber Crime and Cyber Warfare Defined

The key to understanding how to appropriately identify the line between a cyber crime and cyber warfare is defining them separately and comparing the similarities and differences. While this seems simple enough, there are a variety of definitions that all have a level of acceptance from experts.

Cyber crime is defined as “offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). These acts include the spread of viruses or other malware, hacking and distributed denial of service (DDoS) attacks” (McGuire & Dowling, 2013). A simpler definition is “a crime committed through the use of information technology” (Janczewski & Lech & Colarik, 2007). For a crime to be considered a cyber crime it must use technology, and it must do something illegal such as spreading viruses and hacking.

Cyber warfare is defined as “a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses” (Janczewski & Lech & Colarik, 2007). While it can be easy to identify when a nation has committed an attack against their target, it can be difficult to identify a nations’ agents. Cyber warfare can also be seen between two countries that are at war with each other.

When looked at separately these definitions seem perfectly accurate. A cyber crime must involve a crime committed with information technology, and cyber warfare must involve a nation or their agents. However, they are extremely similar. There is a plethora of what-if cases that fall straight into the grey area. For example, what if a nations’ agent attacks a private organization in another country? Is that a cyber crime,

or is that cyber warfare? This is the issue. While these definitions are descriptive separately, when put together they leave a lot up to interpretation when trying to find the line between cyber crime and cyber warfare. This makes it extremely difficult to develop laws. Lawmakers are not experts in cyber crime, so they look to experts in the field to make the most informed laws as possible. When experts disagree with each other the laws will still have similarities, but the grey area will remain undefined.

Cyber Crime Examples

Data breaches are a common form of cyber attacks. The following examples are classified as cyber crimes because these specific attacks were committed against private organizations. A cyber attack is often classified as a cyber crime when no government entity is involved.

Data breaches happen because of lack of security on a company website. The attacker can steal a vast amount of customer information in a very short amount of time. The information stolen ranges from names to credit card information. If a hacker can obtain credit card information from just a few thousand people, a lot of damage can be done; millions of dollars could be stolen. It is important to understand what went wrong in major data breaches of large corporations. There are five major data breaches that will be discussed; they are eBay, Equifax, Home Depot, JPMorgan Chase, and Target. Each one has been hit with a data breach that resulted in customer information being stolen.

When studying data breaches there are a few important questions that must be asked and answered to prevent future data breaches. When did it happen? When was it discovered? How many customers were affected? What was stolen? How severe was it? What did customers need to change? Was any money stolen? Did the company have to pay any settlement? If known, how did it happen?

This last question is the most important for cyber security teams because if it is known how the attacks happen, future attacks can be stopped by upgrading the security protocols for the system. They can also create variations of the protocols to stop similar attacks from hitting the company in the future.

eBay Data Breach

The eBay data breach happened between late February and early March of 2014 (Kelly, 2014). It was later discovered in May of the same year which means that the attack went unnoticed for about a month. This is not uncommon because when an attack goes undetected, it often takes a long time for it to be seen and stopped. Relatively, a month is a short period of time for the attack to be detected.

The number of affected customers is unknown, but as a precaution, eBay told all its 145 million customers to be alert (Kelly, 2014). This was the safest and smartest thing for eBay to notify all its customers. Since the number was unknown, it would not have made sense for the company to only notify a portion of their customers.

There was a range of information that was stolen including: names, email addresses, physical addresses, phone numbers, and dates of birth (Peterson, 2014). Typically, this information is stored together on the same server. Once a hacker gets into the server, all this information is vulnerable. Luckily, no credit card or monetary information was stolen.

Customers were asked to change passwords as a precaution. This is because with the above information being stolen, an attacker could create a fake account pretending to be a customer. This could affect the customer because it would mean that eBay would think they would have two accounts.

No money or credit card information was stolen. The reason was because all that information is encrypted on a separate server. Even if the attacker had been able to break through that server the information would have been useless until they could unencrypt it. In eBay's case, they partner with PayPal which means that credit card

information is stored behind two separate servers. Since no money was stolen, eBay did not have to pay any settlement.

The attack most likely happened because of what is known as social engineering. An attacker would pose as an employee of (in this case) eBay or an employee of a third-party company that works with eBay. The hacker would send an email to a few real employees of eBay requesting specific credential information. Once the email was opened, malware would be installed into the computer system of eBay and the attacker would now have access to that part of the eBay network. It is estimated that around 100 employees of eBay fell into the trap (Peterson, 2014).

Equifax Data Breach

Equifax is a credit reporting agency that allows their user to know what their credit score is. They are one of the largest in the country. The Equifax data breach happened in Mid-May of 2017 (Johnson, 2018). It was later discovered in July of the same year.

It is estimated that around 143 million customers were affected. For perspective, they have around 800 million customers. This is a very large percentage of their customers affected.

Critical information was stolen from Equifax about their customers. Names, dates of birth, social security numbers, addresses, phone numbers, email addresses, and payment cards were all stolen from at least a portion of the 143 million customers (Johnson, 2018). Of the information stolen the most important is the credit cards.

Data Element Stolen	Standardized Columns Analyzed[1]	Approximate Number of Impacted U.S. Consumers
Name	First Name, Last Name, Middle Name, Suffix, Full Name	146.6 million
Date of Birth	D.O.B.	146.6 million
Social Security Number[2]	SSN	145.5 million
Address Information	Address, Address2, City, State, Zip	99 million
Gender	Gender	27.3 million
Phone Number	Phone, Phone2	20.3 million
Driver's License Number[3]	DL#	17.6 million
Email Address (w/o credentials)	Email Address	1.8 million
Payment Card Number and Expiration Date	CC Number, Exp Date	209,000
TaxID	TaxID	97,500
Driver's License State	DL License State	27,000

Figure 1 source: Johnson, 2018, this is a chart showing the information stolen and how many people it affects.

The credit card is the most important because based on the chart, over 200,000 people were affected. This means that if only $1000 was stolen from each customer, $200 million dollars would be lost. This is very critical because the attacker would not just spend $1000 per stolen card; they would spend as much as possible resulting in potentially billions of dollars lost.

Customers were told to change their passwords, but it does little for those who had information already stolen. As compensation, Equifax did offer free identity theft protection and credit monitoring services. This was there way of paying a settlement.

This attack happened through software vulnerability. A well-known software called Apache Struts is used by corporations. This tool is an open-source application used to create Java web-based sites (Johnson, 2018). It is unknown as to whether this vulnerability was new or old. If it was old, then Equifax really dropped the ball in terms of patching the system. A new vulnerability is very hard to detect without any incident preceding the knowledge of the faulty software. As a rule, it is safer to assume that third party products contain vulnerabilities that will need to be patched.

Home Depot Data Breach

Home Depot is one of the largest home improvement stores in the country. They supply everyone, from the everyday consumer to construction companies. They are also part of the S&P 500, so they have the means to ensure that their online assets, websites, and customers are secure.

The Home Depot data breach occurred in April 2014 and it was discovered in September of the same year (Winter, 2014). So far, this is the longest interval of time between the estimated attack date and the detection of the attack.

In total, around 56 million customers were affected (Winter, 2014). This is a much smaller number than the first two discussed, but the information stolen from these customers is worse. Customers were told to be alert and monitor the credit cards.

Of the 56 million affected, all of them had their credit card information stolen, and 53 million had their email addresses stolen. This means that if $1000 was stolen from each of the 56 million credit cards, a total of $56 billion would be lost. This is an exponential increase in possible damage done. Luckily, the breach only cost $62 million. While this is a lot of money, the damage could have been a lot worse.

In response, Home Depot did offer affected customers free identity-theft protection and a year of free credit monitoring. This is a nice gesture, but why did the attack happen in the first place? What caused this one to lose so much money?

Attackers were able to obtain third party credentials. This means that the hacker was able to obtain credentials from a company that Home Depot works with. Once the attacker had this information, they were able to pose as someone from the other company and send phishing emails to Home Depot employees asking for help with

some made-up problem. Once the email was opened, malware was installed onto the Home Depot system and it stole customer information and sent it back to the hacker (Winter, 2014).

JPMorgan Chase Data Breach

JPMorgan Chase is the largest bank in America by assets. Being a bank, they should have good security because they are entrusted with working people's savings and retirement funds.

This data breach happened sometime in the spring of 2014 (Reuters, 2014). They were not able to figure a specific month. It was discovered later in August. This means that at most, the breach went unnoticed for about six months.

83 million customers were affected, with about 7 million of them being businesses. This means that more than just 83 million could be affected because of the business' records.

Information that was stolen includes names, addresses, phone numbers, and email addresses (Reuters, 2014). Luckily, there was no evidence of any stolen account numbers, passwords, user IDs, or social security numbers. This means that the hackers were not able to access any of the monetary accounts at JPMorgan Chase.

No money was stolen, but customers were told to be alert and monitor their accounts. Chase said that passwords do not need to be changed because there was no evidence that supported the decision to change passwords. No free credit monitoring was offered, and no type of settlement was needed. What caused this data breach?

Being a large corporation, they have multiple servers that they use for a variety of information. They were applying security updates to all their servers, but one did not get the update (Reuters, 2014). The update included what is called two-factor authentication. This is used by companies to verify that you are who you say you are. For example, when a person logs into a website, they may be asked to provide another way to authenticate that they are the person logging into the account. Without the security update to this one server, hackers were able to sneak into the Chase server and steal customer information.

Target Data Breach

The Target data breach happened in November of 2013. It was later discovered in early 2014 (McCoy, 2017). This is also a relatively short time interval compared to other data breaches because it only took a few months to detect that something was wrong.

In total, 61 million customers were affected with 41 million of them being credit card holders (McCoy 2017). This means that 41 million credit cards were stolen and could be used for a malicious purpose. If the hacker spent $1000 per credit card, $41 billion would be lost.

Information that was stolen includes names, phone numbers, email addresses, credit cards, and dates of birth. The most important of the data is of course the credit cards because stolen credit cards can do the most damage.

Customers were told to monitor their cards and to change their Target Passwords. Millions of dollars ended up being stolen. This is a small price compared to the theoretical $1000 per credit card scenario.

Target was sued by 47 states and the District of Columbia. Target had to pay an $18.5 million settlement and pay affected customers up to $10,000 each based on evidence of stolen money. They also had to provide free credit monitoring to their affected consumers (McCoy, 2017).

This breach happened when an attacker obtained third party credentials. They used those credentials to gain access to Target's system. Once the hacker was in the system, they installed malware in the servers and stole customer information (McCoy, 2017).

Totals

In total, millions of people were affected, and millions of dollars were lost to the malicious attacks. Data breaches provide warnings to other corporations to make sure that their security is up to date and that it is the best that it can be. They also provide a great way to think about how to update security so that the same attack and similar attacks cannot happen again.

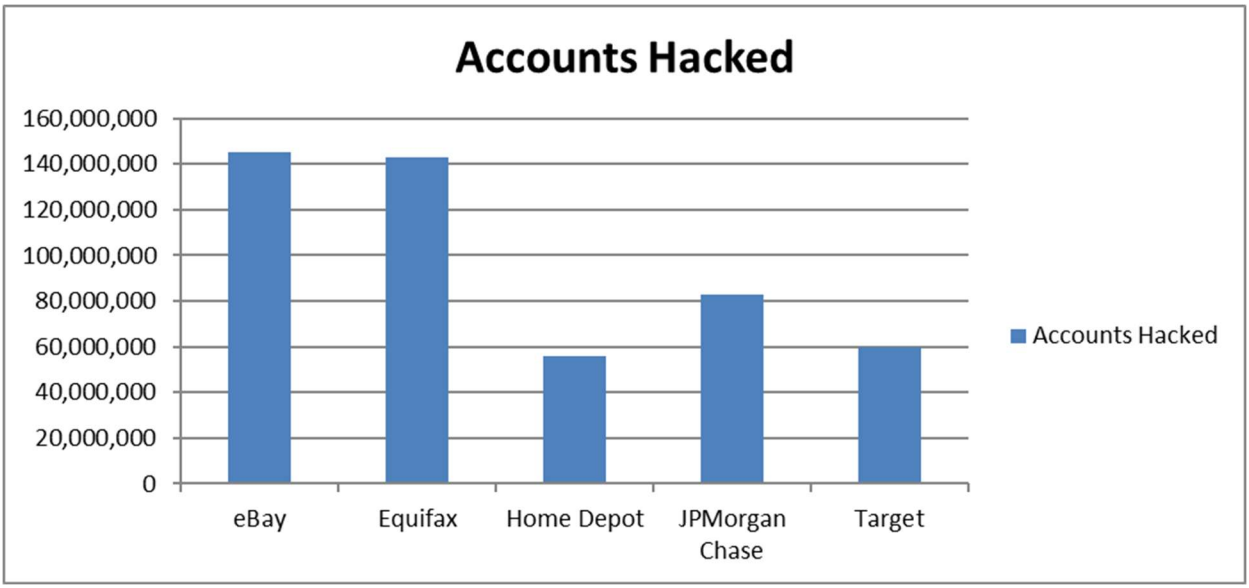

Figure 2 source: Self-created. This chart shows each corporation discussed and the millions affected by each data breach.

Cyber Warfare Examples

Now that cyber crimes have been discussed it is time to look at cyber warfare examples. Cyber warfare must involve a nation either as the perpetrator or the victim. If a nation is not involved in some way, then it is not an act of cyber warfare. The following have been classified as cyber warfare attacks because nations were involved either as the attacker or the victim. The first is the Solar Winds attack that occurred in 2020, and the second is an attack that crippled Iranian internet.

The Solar Winds attack received a lot of attention nationwide. Solar Winds is an Information Technology company based in Texas (BBC, 2020). They provide network management software to many organizations and government entities across the country. The software at the source of the attack is SolarWinds Orion which is a monitoring and management platform “designed to simplify IT administration” (BBC). This attack is thought to have affected 18,000 customers that use Orion. Experts believe that the purpose of the attack was to steal information rather than inflict damage (BBC). The United States departments of energy, treasury, state, defense, commerce, and homeland security were all affected. Former Secretary of State Mike Pompeo stated he blames Russia for what is being described as the worst-ever cyber espionage attack on the US government (BBC). This is clearly an act of cyber warfare because the United States is the victim and based on the definitions, a nation must be involved in an attack for a cyber attack to be considered an act of cyber warfare.

NetBlocks is an internet observatory, which maps internet freedom and volume in real-time, confirmed that there was an extensive disruption to Iranian telecommunications services (Winder, 2020). They reported that internet volume and

activity dropped by 75% because Iranian authorities activated a cyber defense called “Digital Fortress” (Winder). Digital Fortress is meant to repel a cyber attack on the country’s infrastructure. According to NetBlocks it was seven hours before normal internet connectivity resumed (Winder). A spokesperson for Iran’s Telecommunication Infrastructure Company (ICT) said a “distributed denial of service attack” (DDoS) had been repelled by the Digital Fortress. A DDoS attack is an attack that continuously overloads a website’s server so that no legitimate traffic can access it. The server is processing so many illegitimate requests that it cannot process any actual requests. The Digital Fortress put a stop to this by shutting down the internet in Iran until the attack could be contained and stopped. DDoS attacks are a common weapon for nations to use to commit a cyber attack on another nation (Winder).

International Law

To understand why the line between a cyber crime and cyber warfare is not defined, it is important to understand the actual laws. International laws are just as important as domestic laws because experts can draw from multiple sources to form a coherent argument for when a cyber crime becomes cyber warfare. There are two major sources that should be looked at. The first is the Convention on Cybercrime (2001) and cyber security laws in France. The reason for including these sources is because the Convention on Cybercrime is a historic international agreement, and France is a member of the United Nations Security Council and is regularly recognized as a leader of the world.

The Convention on Cybercrime, which is also known as the Budapest Convention, is a historic international agreement. It was the first agreement aimed at reducing computer-related crime by attempting to harmonize national laws, improve investigative techniques, and increase international cooperation (Georgetown Law, 2021). Its main objective is “to pursue a common criminal policy aimed at the protection of society against cyber crime, especially by adopting appropriate legislation and fostering international cooperation” (Georgetown Law). It was passed in 2001 and later adopted in 2004. The importance of “harmonizing national laws” was recognized at the early stages of computer technology. To have the best understanding of how to address computer related crimes, countries must have similar laws that deal with similar or the same issues. This agreement helped lay the foundation for future international and domestic laws that had to address cyber crime and cyber warfare.

France (as stated above) is a leader of the world. They have various cyber laws and related objectives. The foremost of their cyber laws is called the “French National Digital Security Strategy” (French Gov, 2015). It states, “Cybercrime, espionage, propaganda, sabotage, and excessive exploitation of personal data threaten digital trust and security, thus calling for a collective and coordinated response based on five strategic priorities” (French Gov). The five strategic priorities are:

- Fundamental interests, defence and security of State information systems and critical infrastructures, essential operators to the economy and society, major cybersecurity crisis
- Digital trust, privacy, personal data, cybermalevolence
- Awareness raising, initial training, continuing education
- Environment of digital technology businesses, industrial policy, export, and internationalization
- Europe, digital strategic autonomy, cyberspace stability

Each of these bullets lays out why cyber security is extremely important domestically and abroad. They talk about defense of the State and private companies, as well as helping the public understand how to better protect themselves. They also talk about how international organizations must cooperate and provide protection in the event of a cyber attack. Cyber crime is taken seriously abroad because international organizations and countries recognize the threats that can come from cyber attacks.

United States Law

The United States is one of the leaders of the world and in cyber space. The US has been the victim and perpetrator of various cyber attacks over the years, and it was one of the first countries to develop laws dealing with cyber crime. There are two major Acts that have been passed by Congress that will be discussed. The first is the Computer Fraud and Abuse Act (1986) and the second is the Cyber Intelligence Sharing And Protection Act.

The Computer Fraud and Abuse Act (CFAA) was the first federal computer fraud law to address computer hacking. The CFAA prohibits intentionally accessing a computer without authorization or in excess of authorization (Hughes, 1986). This is a vague statement because “in excess of” does not have a concrete definition; it is left up to interpretation. Credit should be given to this Congress because they recognized the threat of computers at its earliest stages. Interestingly, this Act does not define what a cyber crime is, but merely says that it is illegal. This Act protects against the misuse of computers and makes it a crime to commit illegal activity using a computer. The CFAA helped to lay the foundation of future Acts and Bills that the US would make law.

The Cyber Intelligence Sharing And Protection Act (2013) was passed by Congress and later revised in 2014. This Act recognized the need for the sharing of information between law enforcement agencies (Rogers, 2013). It understood that cyber attacks occur every year, even every day, and it may be hard for law enforcement to keep up (Rogers). This Act allows agencies to share data between operational centers to help fight the threats. The Act also helps protect the American people, prevent further

incursions, mitigate damage, and help law enforcement agencies respond and recover from attacks (Rogers).

Motivations for Cyber Attacks

There are a surprising number of reasons why someone or a nation commits a cyber attack. Motivations range from monetary gain to recognition, religion, and more. Some of the major motivations will be discussed.

Monetary gain is one of the most obvious motivations for committing a cyber attack (McAfee). As demonstrated in the Cyber Crime Examples section, there is the potential to gain millions of dollars if the right information is stolen. People that have the right skills can make a quick buck if they execute the attack in the right way against the right target.

Another motivation is recognition; some hackers want to make a name for themselves so they will attack high profile targets such as government entities or large businesses to get their name in the news (McAfee). This type of person will usually try and cause some damage to the target to make sure that the attack gets on the news.

The next motivation for a cyber attack is to cause damage. This usually results from someone being wronged by someone else, so they want revenge (McAfee). Causing damage may mean monetary damage or causing the network to go down for a period of time.

The final motivation to be discussed is religion. Just as those that committed the 9/11 attack claimed it was for religious reasons, so to can cyber attacks be committed for religion (McAfee). Often, attacks with religious motivations stem from political strife either between two nations or within one country.

Motivations for a cyber attack are wide-ranging, so experts and lawmakers must be prepared to defend against all types of attacks.

The Line Between Cyber Crime and Cyber Warfare

Can a line between cyber crime and cyber warfare be established? The simple answer is yes. However, there are a few things that need to happen first. With the current definitions and laws, it is quite easy to tell when a cyber crime or cyber warfare occurs. However, there is a wide grey area between the two. For example, how would an attack on a private organization from an individual in a different country that has ties to the leadership in that country be categorized? This is the grey area that must be defined.

Another example is what about when an individual attacks a government? Until the definitions of both cyber crime and cyber warfare are worked out in a way that is agreeable to most experts this will continue to remain a grey area. Without these specific definitions that address the grey, lawmakers cannot begin making laws that address cyber crime and cyber warfare separately. If lawmakers are unable to create laws domestically, then it will be that much more difficult for international organizations such as the United Nations to address the issues. It all comes down to the definitions.

The line between cyber crime and cyber warfare will eventually be established, but it is new terrain. New terrain takes a great deal of effort to work through, but eventually it will happen. The line is currently grey, but it will be black and white in the future.

References

BBC. (2020, December 19). US cyber-attack: Russia 'clearly' behind SolarWinds operation, says Pompeo. BBC News. https://www.bbc.com/news/world-us-canada-55374945.

France Gov. (2015, October). French National Digital Security Strategy. https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

Georgetown Law. (2021, March 12). International and Foreign Cyberspace Law Research Guide: Treaties & International Agreements. Guides. https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478.

Hughes, W. J. (1986, October 16). H.R.4718 - 99th Congress (1985-1986): Computer Fraud and Abuse Act of 1986. Congress.gov. https://www.congress.gov/bill/99th-congress/house-bill/4718.

Janczewski, Lech, and Andrew Colarik, eds. Cyber warfare and cyber terrorism. IGI Global, 2007.

Johnson, A. (2018, May 8). Equifax breaks down just how bad last year's data breach was. Retrieved April, 2019, from https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496

Kelly, G. (2014, September 02). EBay Suffers Massive Security Breach, All Users Must Change Their Passwords. Retrieved April, 2019, from https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/#7718155c7492

McAfee. (2018, March 16). 7 Types of Hacker Motivations. McAfee Blogs. https://www.mcafee.com/blogs/consumer/family-safety/7-types-of-hacker-motivations/.

McCoy, K. (2017, May 23). Target to pay $18.5M for 2013 data breach that affected 41 million consumers. Retrieved April, 2019, from https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

McGuire, Mike, and Samantha Dowling. "Cyber crime: A review of the evidence." Summary of key findings and implications. Home Office Research report 75 (2013).

Peterson, A. (2014, May 21). EBay asks 145 million users to change passwords after data breach. Retrieved April, 2019, from https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/?noredirect=on&utm_term=.a2205c90c4a5

Reuters. (2014, October 03). JPMorgan hack exposed data of 83 million, among biggest breaches in... Retrieved April, 2019, from https://www.reuters.com/article/us-jpmorgan-cybersecurity/jpmorgan-hack-exposed-data-of-83-million-among-biggest-breaches-in-history-idUSKCN0HR23T20141003

Rogers, M. J. (2013, April 22). H.R.624 - 113th Congress (2013-2014): Cyber Intelligence Sharing and Protection Act. Congress.gov. https://www.congress.gov/bill/113th-congress/house-bill/624.

Winder, D. (2020, February 9). Powerful Cyber Attack Takes Down 25% Of Iranian

Internet. Forbes. https://www.forbes.com/sites/daveywinder/2020/02/09/powerful-iran-cyber-attack-takes-down-25-of-national-internet/?sh=5132929e20dc.