The International Conference on Interdisciplinary Humanities and Communication Studies
DOI: 10.54254/2753-7048/4/2022550

Cyber Warfare & Terrorism

Yang Zhang[1,a,*]

[1]Fossil Ridge High School, Fort Collins, USA
a. Carrlisa2080@gmail.com
**corresponding author*

Abstract: The cyberspace is arguably one of the most dangerous and safest places on earth. In a second you can trust the companies you shop at or provide the information to keep them safe, but the next second a data breach could be carried out on the company you trusted. There's nowhere as long as you're on the internet that's 100% safe and hack prove. Especially when online criminal activities are cheaper to carry out, the same as buying and selling illegal products, wars also carry into the cyberspace as well, and recently the Idea of cyber terrorism was introduced.

Keywords: Cyber-attack/warfare, Cyber terrorism, Cybercrime

1. Introduction

Ever since the creation of the internet, a new type of crime has emerged from the shadows: cybercrime. From thrill-seeking to effecting computers with malware, online criminals are finding more and more ways to steal, purchase illegal items, and rob. Or even worse, organize group attacks that can intervene/mess with governmental defense and weakening the security of our nation. In recent years cyber warfare aka. Information warfare and cyber terrorism have been on the rise, and nations have put in some efforts to prevent havoc from breaking loose. However, cybersecurity is a field where the attackers have the advantage with little to no general public knowledge. The purpose of this essay is to inform the public about the danger of cyber-attack/warfare, cyber terrorism, and call for more research in the future to help prevent havocs caused internationally over the internet.

2. Ease of Use

This paper is divided into two main sections and the two main sections are divided into two sub-sections. The first section will be about cyber warfare, with the three subsections talking about what is cyber war crime, some examples, and what people should do to secure their information better. The second section would be about cyber terrorism, with four different subsections talking about what cyber terrorism is and difference between physical and cyber terrorism, a few hypotheses about what it'll look like and call for more research to take place.

2.1. What is Cyber Terrorism

Cyber terrorism is a new form of terrorism that first originated in the 1980s, it is structurally and conceptually very close to cyber warfare. However, the activities are done by terrorists with the intention of bringing down the US and a few other countries instead. There are currently two types of cyber terrorism, one targeting and attacking Data, and the other trying to hack in and control systems for a greater damage. Instead of carrying shoe bombs, technology have developed to a rate that even small terrorist organizations have the resources to put together computers and plan online for their next move. And because computers and the concept of cyber warfare and terrorism is so new, there aren't many laws that are passed against them. The closest being against individual terrorists or small group at a time. The problem with cyber terrorism is that it is unpredictable, and could be caused by any organization or person, even by someone you trust dearly.

2.2. What is Cyber Warfare

Cyber warfare is a new way that more nations have to adapt to since it started in 2003 within the cyber space. Involving adversaries launching attacks on the main infrastructure of the country they're targeting, including transportations, water supply system, gas and oil storage and delivery, banking and finance, government operations, communications, emergency service and energy [1]. Cyber-attacks used in cyber warfare includes trojan horses, denial of service, worms, sniffers, logic bomb, and viruses, sometimes it will be in combinations. The attackers can be anyone, ranging from government organized group attacks, hired hackers, illegal organizations, terrorists, gangs, and mafias to personnel in cybersecurity, civilian hackers, and general people who know the internet system [2]. Launched between countries, the offensive side of cyber warfare are constantly trying new methods to sabotage their enemies, such as vandalism, collection of data, network & none internet-based attack against infrastructures, Access of Denial attack, and propagandas [3,4,5]. The damage this attack can cause could deal varies, from little temporary shortages and alterations to shutting down supplies [6]. Furthermore, because of the high connections within the cyber space, the attacks can be launched traceless from anywhere across the world. Companies are risking a chance that an angry employee leak documents to the public, hackers around the world can fake to be a part of the government and spread misinformation while launching a group attack on the government [7].

2.3. C. Examples of Cyber Warfare

2.3.1. The First Case if Cyber Warfare

Hybrid warfare on Estonia [8]. In 2007 two waves of DDos attacks were launched at Estonia, the second wave being more devastating than the first, after the government revealed their intention of moving a Soviet-war memorial site. When the protesting against the moving of the soviet memorial site started, a two-night looting and riot broke out, which in turn sped up the process of removal. Soon after, the protesting died down, and in place of the protest was a wave of well-coordinated cyber-attack which immediately threw Estonia into havoc. The attack stared on May 4th and reached its peak on victory day, the attacks were so coordinated, in fact, that it was planned in a way that not a single time period did the attacks clam down, and the attacks changed as countermeasures were put in. Adding on top of none-stop cyber-attacks flooding the servers of the parliament, large telecommunication companies, and two major banks, adversaries also hijacked the railway system [9].

Because most of the IP address during the attack, and the coordinated instructions are either in Russian or from Moscow, Russia was immediately blamed for starting and supporting the cyber-attacks. However, ambassadors from Moscow claimed that Russia itself was dealing with their own trouble, during the same time cyber-attacks were also launched at Russia. There were no solid evident on both sides, therefore no country was charged by NATO [10].

Both ways, this hybrid warfare served as a wake-up warning to NATO and all of the countries on how fast attacks can be pulled off without a solid trace in daylight. And laid the framework of how cyber warfare and cyberterrorism. Soon after, Nato laid out new frameworks on the first set of defenses against cyber warfare and terrorism [11].

2.3.2. Hybrid Warfare on Georgia

Soon followed the attack on Estonia, Russia immediately jumped into attacking another country, which is the hybrid warfare on Georgia. the attacks were launched in 2008, just less than a year from the attack on Estonia. By July 20th, there were already large cases of zombified computers scattered around Georgia. Due to the attacks, the president's website was hit by overflow errors and the servers redirected users to a different site where the loading screen stated “win+love+in+Russia" And then the site was taken down for the next 24 hours. At the same time, Turkey, which boarders Georgia pipeline was also under terrorism attacks. The blame for the terrorist attack was originally on the PKK, however there’s evidence suggesting that it was an online computer attack that took control of the pipeline's safety system, which indirectly caused the pressure to build up, in turn led to the pipeline exploding.

On Aug. 9 just less than four days after the pipelines exploded, most websites in Georgia were redirected to imposter webpages and were sent through a lot of foreign servers. The servers are shown to be located in Moscow, the capital of Russia. German companies at the time sided with Georgia and moved most government infrastructure to their private network. Despite the efforts to put in new security and private connection, most websites in Georgia at the time faced major attacks and denial of service, and within hours the networks were running based on Russian servers again. On the 10th a counter attack from Georgia was launched against RIA News Agency, disabling their web servers. The agency’s IT department stated that both their websites and DNS-servers were under server cyber-attacks. At the same time, Jart Armin warned the public not to trust any official Georgian websites as they could be imposter fraud sites. Jart Armin also warned that the news published about Georgians can’t be trusted within the attack time. Because they could be fraudulent posted by the attackers.

Aug 11, 2008, the president of Georgia picture on the website have been altered and defaced, with the image comparing him to Adolf Hitler. At the same time the parliament have also been targeted, adding on top of everything, commercial websites are facing crashed servers and their websites are being taken down for no reason. On the same day, Georgia declared and accused Russia for all of the trouble they’ve been causing and waging a hybrid Warfare [12]. However, the wrong doings were denied by the spoke person from Russia claiming that Moscow was also under cyber-attacks.

As the result, the web pages were moved to US servers and the government of Estonia also offered help [13].

The relationship between cyber-attacks, cyber terrorism, and cyber warfare is sometimes a gray area. However, it is also quite similar to the relationship between squares and rectangles. Both cyber warfare, and cyber terrorism uses cyber-attacks, but not all cyber-attacks are acts of cyber warfare and cyber terrorism. At the same time, it doesn’t take a cyber terrorism to trigger a cyber warfare, and cyber terrorism can be a part of a cyber warfare. With that being said, well-coordinated and designed cyber-attacks are the main frame for cyber terrorism and cyber war fair which leads to our next part.

2.4. D.Types and Examples of Cyber Attacks

2.4.1. Wanna Cry?

On May 12th, 2017, organizations across the word weren’t ready for a new type of cyberattack. Wanna cry, a ransomware built with both the property of a worm and a malware. Within a few months, Wanna cry became one of the most notoriously destructive and widespread cyber/malware-attacks in history. Even though has been five years since the start of the attack, thousands of computers are still getting infected around the world. The malware itself have over twelve thousand different variants and the only way to remove it from a computer is to use a known domain to trigger the kill switch of the malware. The kill switch is a very unique distinct feature that Wanna cry has that researchers yet have the answer to why it was there.

The malware attacks all started on the 12th of May in 2007, It quickly speeded across the world, infecting more than 200000 computers alone, excluding all other computing devices. Hundreds of thousands of people were affected by the ransomware and got locked out of their computer, with the page usually stating that the files have been encrypted and they need to pay a ransom to get it unencrypted. The fee of decrypting the code cost usually around 300 dollars in bitcoins, which doubles after a certain time period, however there is a chance that you'll still lose your files after paying the ransom. Later the stakes got raised to 600 dollars' worth of bit coin at the start, and the documents will be erased if the ransom wasn't paid for. Other than attacking regular civilians and average joes, Wanna cry also targeted large corporations and governmental infrastructures like the British National Health Service.

The exploit Wanna cry was using is the exploit called eternal blue, which was patched in the brand-new windows update at the time, however most computers weren't keeping up on the update, which leaded to millions of computers vulnerable to the attack. The exploit itself was actually a stolen piece of information that was leaked by The Shadow Brokers. Which allowed Wanna cry to spread through remote computers. Adding on top of that, the worm like behavior of Wanna cry made it so that the ransomware can spread through computers on its own, send malicious emails containing a copy of itself, and send the ransomware to random IP addresses in order to affect that device.

Wanna cry continues to spread through the world and left hundreds of thousands of computers with all content erased, and millions of users, regardless of whether they're IT specialists, students, or workers, leaving large corporations and cybersecurity specialists/ researchers in frustration. That was the case before 2 researchers in the United Kingdom, Jamie Hankins and Marcus Hutchins caught on to something suspicious within the malware. A strand of code which included a few domains that can stop Wanna cry from attacking, and command it to "self-destruct" within the device, which means that the attack will stop dead as soon as the live domain was detected. Which ended the attack effectively after the publication on May 12th in 2017 [14].

Wanna cry's ability to encrypt all types of documents and have the ransomware with multiple language action is also a main reason for its effectiveness other than the worm like property. when a computer is infected and attacked, Wanna cry will drop a file named! Please Read Me!.txt which contains the instruction to pay the ransom. The instruction is available in 28 different languages that are most commonly spoken. If that isn't stunning enough at that time period, Wanna cry can also encrypt around 228 types of files. Including virtual machine files, digital certificates, graphic files, office files, national specific formats, archives, emails and their corresponding databases, media, encryption keys, photography files, developer project files, database files and source codes.

However, just like every other cyber-attack, Wanna cry also has a counter attack strategy for both individuals, and organizations. The best way to prevent from getting infected by Wanna cry on the individual level is to block the spams, routinely back up all of the critical information you have in order to prevent further complications. In case of a Wanna cry infection, the best way of backing up is to store the information on a different device offline, Disabling macros within Microsoft office products, avoid opening unsolicited e-mails and it's attachments even if it's from someone in your contacts, as it might be an attempt from their infected devices to spread the virus. At last, the most important step, deploy and constantly update an antivirus program on your device so that you get notified when something goes off [15].

2.4.2. Morris Worm

On the 2nd day of November, a period of chaos began. Morris worm, the first computer worm is on the attack. The product wasn't an intentional attack from the enemy nor a test to show the strength of computers, but instead, it was written by a grad student. As the cyber worm continued to spread, tens and thousands of computers were affected at the time, which as a result brought out great panic. The attack started out as small local attack, but it soon became one of the most well-known attacks in history as it slowed the computers it infected [16].

The worm's targets all had something in common, that is they all use the Unix operation system. However, that's not the only way of getting inside. This cyber worm can also get in by using a bug in the finger program and the back door of email. The cyber worm didn't destroy any files, which was a good thing. Out of concern many institutions wiped and disconnected their computers from the internet for a week. Many emails are lost and wiped with all other data's as well. The solution to this cyber worm is then developed by researchers to effectively deal with the incident.

The person that started the cyber worm actually contacted two of his friends and expressed his sorrow for the incident and attached the solution to the email he sent. despite the computers being slowed down so much, the email still went through the computers and got received in time to help stop the worm. His friends sent both the solution and apology letter to new York's time on his behalf, using the letters of the culprits' name. As soon as that piece of information was leaked, the FBI's investigation hit the ground running. And the culprit was indeed Robert Tappan Morris, a grad student at MIT.

Surprisingly, Robert did break a federal law at the time. According to the Computer Fraud and Abuse Act, he gained unauthorized access to computers that wasn't his, the indication was in 1989, and he was found guilty by the jury in the following year, which made him the first person to be charged under the law. Surprisingly he didn't get any time in jail, instead, he was charged with probation, received a fine, and did 400-hour worth of community service.

The total damage for the Morris worm was estimated to be around 100,000 dollars up to millions, this event was a wakeup call for cyber security, and network safety [17].

2.4.3. Ways to Prevent a Cyber Attack

Though the effect sound grim, there's no need to be anxious about large-scale cyber warfare. Ever since the first attack recorded by the government in 2003, the government started to turn their funding toward the cyber security aspect of the defense, including the FBI, CIA, NETCOM, NSA, DHS, CYBERCOM, and branches of the military. Spending about 37 billion dollars a year on IT and about 5.4 billion dollars on Cybersecurity, there for you don't need to worry about large-scale group attacks. However, as an average person there's a few ways to protect your own data and keep it safely stashed away from the hackers [18]. To start with, phishing and spear smishing, in those cases adversaries are pretending to be an important sender through emails. Some characteristics of a phishing email are that they usually are marked as a time sensitive mail, there might be grammatical and spelling errors, they sometime will ask for more of your information and send you malicious web site and files. The easiest ways to prevent that is to remove any emails that seem suspicious, have all of your antivirus software up to date, report these incidents, and report them to the FSO [19]. In case of a brute force attack, use a lock feature where your account would freeze after a certain number of attempts, and you have to be an authorized person, in this case, the user, to unfreeze the account. And last, but not least in case of a dove by attack, make sure that all the website you go to have the little lock symbol and is well secured as the hackers can inject a malware into a less secured website and infect your device once you clicked on and opened the website[20].

3. Conclusion

Even though there's no guaranteed safety within the cyber space, it is likely to become a bigger part of our future. What we really need to do is to conduct more research and gain higher ground in terms of digital defenses. Since cybersecurity is a job where you secure others' data online and build defenses around new inventions and scientific advancements so that the criminals would get their hands on/in to their security systems and cause havoc. As from the examples provided in this article, more attacks and cyber warfare will happen, and the only way we can defend ourselves and our country are to be ready.

References

[1] *"5 Top Cybersecurity Threats & Their Solutions for 2020." Straight Edge Technology, Inc., 25 Nov. 2019, www.straightedgetech.com/5-top-cybersecurity-threats-and-their-solutions-for-2020/.*

[2] *Akujuobi, Cajetan. "Cyberterrorism." Reaserch Gate, Oct. 2016.*

[3] *Bhuyan, Soumitra Sudip, et al. "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations." Journal of Medical Systems, vol. 44, no. 5, Apr. 2020, https://doi.org/10.1007/s10916-019-1507-y.*

[4] *" Cyberattacks during the Russo-Georgian War - HandWiki." Handwiki.org, handwiki.org/wiki/Cyberattacks_during_the_Russo-Georgian_War. Accessed 16 Sept. 2022.*

[5] *Federal Bureau of Investigation. "Morris Worm." Federal Bureau of Investigation, www.fbi.gov/history/famous-cases/morris-worm.*

[6] *Fortinet. "Top 20 Most Common Types of Cyber Attacks." Fortinet, www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks.*

[7] *Ginter, Andrew. THE TOP 20 CYBERATTACKS on Industrial Control Systems. 2018, www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf.*

[8] *---. THE TOP 20 CYBERATTACKS on Industrial Control Systems. 2018, www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf.*

[9] *Hrůza, Petr, and Jiri Cerny. "Cyberwarfare." Reaserch Gate, 1 Oct. 2017, www.researchgate.net/publication/318737253_Cyberwarfare.*

[10] *NSA'S Top Ten Cybersecurity Mitigation Strategies. www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf.*

[11] *Rapid7. "Common Types of Cybersecurity Attacks and Hacking Techniques | Rapid7." Rapid7, 2018, www.rapid7.com/fundamentals/types-of-attacks/.*

[12] *Ray, Fagan. CYBER WARFARE WHAT'S REALLY HAPPENING? www.grandcomputers.org/Documents/TechSig/CyberWarfareRayFagan.pdf.*

[13] *SophosLabs -WannaCry Aftershock 1. www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf.*

[14] *Srikrishna, Devabhaktuni. Cyber Warfare: Surviving an Attack. pubs.fas.org/_docs/2010_Fall_Cyber_Warfare.pdf.*

[15] *Swinhoe, Dan, and Michael Hill. "The 18 Biggest Data Breaches of the 21st Century." CSO Online, 16 July 2021, www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.*

[16] *"The Biggest Cyberattacks in History." History Hit, www.historyhit.com/the-biggest-cyberattacks-in-history/.*

[17] *"The Biggest Cyberattacks in History." History Hit, www.historyhit.com/the-biggest-cyberattacks-in-history/.*

[18] *The Russo-Georgian War 2008. 2012, www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.*

[19] *Wannacrypt, Wannacry. CRITICAL ALERT. www.csk.gov.in/documents/WannacryWannaCryptRansomware_CRITICAL_ALERT_CERT-In.pdf. Accessed 16 Sept. 2022.*

[20] *White, Sarah. Understanding Cyberwarfare Lessons from the Russia-Georgia War. 2018, mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.*