International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:07, Issue:10 "October 2022"

HOW CYBER WARFARE CONTROLS MODERN-DAY CROSS-BORDER POLITICS

Abhinav Chaudhary

Delhi, India

DOI: 10.46609/IJSSER.2022.v07i10.008 URL: https://doi.org/10.46609/IJSSER.2022.v07i10.008

Received: 4 October 2022 / Accepted: 15 October 2022 / Published: 28 October 2022

ABSTRACT

Cyber warfare allows a nation to weaken, disrupt and destroy enemy nations by attacking them in cyberspace without putting any actual human lives on the line. Today, all systems and individuals have become interconnected and interdependent to a point never imaginable before. Further, the military's reliance on computers and network systems has also increased exponentially.

While this interdependence and interconnectivity provide various workflow advantages, it also makes these networks a ripe target for cyber attacks. These attacks are capable of disrupting a nation's most critical civilian systems namely communication, finance, healthcare, transportation, etc. as well as military systems. These matters concerning national security have made cyberspace a subject of high political importance.

Cyber-attacks and cyber-warfare have entered the arsenal of modern warfare and being preemptive by setting up enhanced defenses against these attacks is our only option.

This research paper aims to analyze and document various instances of cyber warfare in the past years. This analysis will help us define what cyber warfare is and its extent. We stand to learn the various approaches taken by different governments to orchestrate such an attack.

Further, we'll try to understand the strategies put in place by various current governments of the world trying to shield themselves from such an attack. Lastly, we'll look into how the advent of cyber warfare will change the world in years to come forcing governing agencies of the world to come up with laws or a single autonomous body to stop cyber warfare.

INTRODUCTION

Throughout history, humanity has been waging wars while seeking to advance its nation's agenda in the ever-changing international game of power. From the fierce battles of yesteryears to today's unmanned drone attacks, technology is constantly changing and evolving this power game. The development of armored vehicles, aircraft, ships, and the use of electronics and telecommunications have all introduced new and innovative ways to expand combat space and gain an edge over enemies. The emergence of cyberspace has led nations to pour resources into developing their cyber arsenal to ensure a dominant position.

What is Cyberwarfare?

Cyber warfare is usually defined as a cyber attack or series of attacks that target a country. It has the potential to wreak havoc on government and civilian infrastructure and disrupt critical systems, resulting in damage to the state and even loss of life.

There is, however, a debate among cyber security experts as to what kind of activity constitutes cyber warfare. The US Department of Defense (DoD) recognizes the threat to national security posed by the malicious use of the Internet but doesn’t provide a clearer definition of cyber warfare.

Cyber warfare typically involves a nation-state perpetrating cyber attacks on another, but in some cases, the attacks are carried out by terrorist organizations or non-state actors seeking to further the goal of a hostile nation. There are several examples of alleged cyber warfare in recent history, but there is no universal, formal, definition for how a cyber attack may constitute an act of war.

History

Even for a country as well developed and established as the United States of America, cyber warfare has been an increasing issue for the past ten years. So much so that upon testing, the government was able to figure out that only two professionals of cybersecurity hacking and proper skills are needed to hack into the private government documents and even gain access to weapons and war material that the country has. Thus making cyberspace one of the biggest vulnerabilities that every nation has had to fight against.

There have been many different noticeable and famous cyber-attacks in the past, which have been mistakes other companies and nations have learned from, as to avoid a repetition of a similar sort of attack. The first attack goes as far back as 2010, when Stuxnet was introduced, which was a cyber-weapon used against Iran to ruin their nuclear weapons and power by having the ability to cause actual physical damage to those nuclear weapons. The next bigone was in 2014, by the Russians and against the Ukrainians, when Russians had a DDoS attack, limiting and removing the internet in the country in an attempt to take control of the country. In the same year, Russian cyber-attackers also took over the presidential campaign, just three days before the election, so that there was chaos everywhere, and everybody would choose to have a Russian leader instead. One of the most recent ones was in 2017, when an attack called 'WannaCry' attacked Microsoft computers in over 150 different countries, affecting the overall status of the company and the reliability of its products.

Types of Cyber Warfare Attacks

There are mainly seven types of Cyber warfare attacks

Espionage

Refers to monitoring other countries to steal secrets. Cyber warfare can involve armies of nefarious hackers from around the globe who use botnets or spear phishing attacks for economic, political, or military gain. These deliberately recruited and highly valued cybercriminals have the technical know-how to shut down anything from government infrastructures to financial systems or utility resources. They have influenced the outcome of political elections, created havoc at international events, and helped companies succeed or fail.

Sabotage

Sabotage is defined as deliberate and malicious acts that result in the disruption of normal processes and functions or the destruction or damage of equipment or information. Cyber Sabotage is another wrinkle in the emerging threats from cyberspace. Whether delivered overthe internet or purposefully installed during the manufacturing process, contaminated hardware or software is now a concern. Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as dissatisfied or careless employees, or government employees with affiliation to the attacking country.

Denial-of-service (DoS) Attacks

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding thetarget with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. This attack occurs when multiple systems orchestrate a synchronized DoS attack on a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once.

Electrical Power Grid

Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.

Propaganda Attacks

Propaganda is an old and effective technique that has been used by nation-states and organizations to manipulate and sway public perception. Modern propagandists have been quick to take advantage of new modes of communication, and also quick to leverage their relative insecurity. They have hacked databases and personal devices, and have also spread messages much more quickly and broadly through social media and online news sites. This more evolved approach has been identified as cyber propaganda.

Economic Disruption

Most modern economic systems operate using computers. Attackers can target computer networks of financial establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

Surprise Attacks

These are the cyber equivalent of attacks like Pearl Harbor and 9/11. The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses. This can be done to prepare the ground for a physical attack in the context of hybrid warfare.

What are the Pros and Cons of Cyber Warfare?

Due to the low cost of setup compared to military operations and no soldier lives at stake cyber warfare has come up to become the preferred mode of war. As more and more countries are suiting up to fight the cyber war we need to consider the pros and cons that come with it.

There are some benefits and some advantages of cyber warfare as a whole. Looking at the benefits first, the biggest one that comes to mind is that nations that are most at risk have greatly developed and invested in their technology departments in order to stay one step ahead of the hackers. This, in general, has made people feel a lot more secure, and even the governments feel a lot less vulnerable to outside and enemy exposure since they have strong defenses up and teams working on keeping the security up-to-date, around the clock. Similarly, another benefit of cyber warfare means that nations are very careful about their sensitive information and have resorted to much more formal ways of conducting the meeting. As it can often be observed, some of the most sensitive meetings take place inside offices that are entirely signal-free, free from technology, and any kind of device which may be hackable.

However, there is no doubt that the cons definitely outweigh the pros, in a way that it creates a very uncertain and unstable situation globally, where anybody's sensitive data could be accessed at any time, without their consent. And like all other situations, in this one too, the poorer and more backward nations suffer the most since they don't have the funding or the resources to set up stronger defenses for their nations. Thus it eventually becomes a game of the developed and richer nations, who can even treat smaller and weaker nations as puppets because of the high level of power they hold over them.

RESEARCH METHODOLOGY

In this paper, we use the method of secondary research to arrive at a conclusion for our implied hypothesis.

Secondary research, also known as desk research, is a research method that involves compiling existing data sourced from a variety of channels. This includes internal sources (e.g.in-house research) or, more commonly, external sources (such as government statistics, organizational bodies, and the internet).

It comes in several formats, such as published datasets, reports, and survey responses, and can also be sourced from websites, libraries, and museums. The information gathered using surveys, telephone interviews, observation, and face-to-face interviews is usually free or available at a limited access cost.

When using secondary research, collection, verification, and analysis of the collected data are done. Data is then incorporated into their research to help them confirm the research goals for the research period.

Advantages of Secondary research

Easily and readily available data – There is an abundance of readily accessible data sources that have been pre-collected for use, in person at local libraries and online using the internet.

Faster research speeds – Since the data is already published and in the public arena, you don't need to collect this information through primary research. This can make the research easier to do and faster, as you can get started with the data quickly.

Low financial and time costs – Most secondary data sources can be accessed for free or at a small cost to the researcher, so the overall research costs are kept low.

Ability to scale up results – Secondary sources can include large datasets (like Census data results across several states) so research results can be scaled up quickly using large secondary data sources.

Disadvantages of Secondary research

Research data can be out of date – Secondary sources can be updated regularly, but if you're exploring the data between two updates, the data can be out of date. Researchers will need to consider whether the data available provides the right research coverage dates, so that insights are accurate and timely

Secondary research needs to be verified and interpreted – Where there's a lot of data fromone source, a researcher needs to review and analyze it. The data may need to be verified against other data sets or your hypotheses for accuracy and to ensure you're using the correct data for your research.

Secondary research data is not exclusive – As data sets are commonly available, there is no exclusivity and many researchers can use the same data. This can be problematic when researchers want to have exclusive rights over the research results and risk duplication of research in the future.

Hypothesis Implied

It is hypothesized that the evolution of cyber warfare as an effective and preferred mode ofwar will have a momentous impact on the ever-changing structure of political power in theworld.

Literature Review

The identification of literature for analysis in this paper was based on a keyword search. These keywords were initially "Cyber War" and "Cyber Warfare" but as subtopics such as cyber weapons and cyber deterrence were discovered, these also became keywords for furthersearches.

The keywords were entered into common internet search engines such as Google, allowing the discovery of articles not indexed in digital libraries. Keeping in mind that cyber warfare is an interdisciplinary subject, articles from other disciplines such as law, international relations, and defense were also searched for relevant sources.

- **What is Cyber Warfare | Types, Examples & Mitigation | Imperva:** This article provided us with a basic understanding and definition of cyber warfare. The author also mentioned the different types of cyberwarfare attacks that can be witnessed in today's scenario with appropriate examples for each of them

- **Cyber Warfare Conflict Analysis and Case Studies**: This thesis provides researchon historical cyber-warfare incidents from the past to current and maps the relevant cyber-warfare data in a well-known framework called CASCON, which is a history-based conflict analysis and decision-support system. The CASCON-based analysis for cyber incidents revealed a larger picture of the world we live in and how easily that world could change.
- **10 Ways to Reduce Cybersecurity Risk for Your Organization | UpGuard**: This article provided insight into practical strategies an organization of a country can implement to safeguard against the risk of cyber attacks.
- **Cyber Warfare in Global Conflicts, by Keren Elazari - SHAPES - Iberdrola:** This article talked about how cyber warfare has affected global conflicts and how theadvent of the cyber age has put everyone on a virtual battlefield. The article providedme insight into how cyber warfare would affect the future of political conflicts and was used to understand how warfare has evolved.

ANALYSIS OF DATA

Case studies

Cyber-Warfare incidents from the past were researched for this paper, included are a number of prominent and publicized Cyber-warfare cases.

Olympic Games (a.k.a Stuxnet)

Stuxnet is a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran. Although neither country has openly admitted responsibility, the worm is widely understood to be a cyberweapon built jointly by the United States and Israel in a collaborative effort known as Operation Olympic Games.

Dispute background

In 2002 an Iranian opposition group revealed that Iran was developing nuclear facilities including a uranium enrichment plant at Natanz and a heavy water reactor at Arak. The US accuses Iran of a clandestine nuclear weapons program, which Iran denies. A decade of intermittent Iranian engagement with the UN's nuclear watchdog and diplomatic activity followed. The UN ratified four rounds of sanctions on Iran between 2006 and 2010 over the nuclear issue. This led to the deployment of the malware, Stuxnet.

Modus operandi

Stuxnet has three modules: a worm that executes all routines related to the main payload of the attack; a link file that automatically executes the propagated copies of the worm; and a rootkit component responsible for hiding all malicious files and processes, to prevent the detection of Stuxnet.

It is typically introduced to the target environment via an infected USB flash drive, thus crossing any air gap. The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC. In the absence of either criterion, Stuxnet becomes dormant inside the computer. If both conditions are fulfilled, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the code and giving unexpected commands to the PLC while returning a loop of normal operating system values back to the users.

Damage caused

Stuxnet specifically targeted programmable logic controllers (PLCs), which allowed the automation of electromechanical processes such as those used to control machinery and industrial processes including gas centrifuges for separating nuclear material. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.

Post Hostilities

Uranium enrichment of the Nuclear program was withdrawn and sanctions were withdrawn.

Personal Opinion

The Stuxnet attack was a highly sophisticated first-of-its-kind attack where computer code was used to disrupt and destroy physical property like the centrifuges. This attack perfectly encapsulates the scale at which a well-executed cyber attack can cause damage to the target country's infrastructure. The US was the non-status quo country here and did not want Iran to develop nuclear facilities in order to maintain its political high ground over the country of Iran.

The Shamoon Attack I & II

Shamoon, also known as W32.DistTrack is a modular computer virus that was discovered in 2012, targeting then-recent 32-bit NT kernel versions of Microsoft Windows. The virus has been used for cyber espionage in the energy sector. It was notable due to the destructive nature of the attack and the cost of recovery. Shamoon can spread from an infected machine to other computers on the network. Once a system is infected, the virus continues to compile a list of files from specific locations on the system, upload them to the attacker, and erase them. Finally, the virus overwrites the master boot record of the infected computer, making it unusable.

Dispute background

The malware was unique, used to target the Saudi government by causing destruction to the state-owned national oil company Saudi Aramco. Hackers calling themselves the "Cutting Sword of Justice" claimed responsibility for the incident, asserting they were retaliating against the al-Saud regime for what the group called widespread crimes against humanity.

U.S. intelligence sources have attributed the attack to Iran. Less than two weeks after the Aramco incident, the Qatari gas giant RasGas was also knocked offline by suspected state-sponsored attackers.

Modus operandi

The virus consisted of three components, the Dropper, the Wiper, and the Reporter. The Dropper, the source of the infection, creates a service with the name 'NtsSrv' that enables it to remain persistent on the infected computer. The Dropper was built in 32-bit and 64-bit versions. If the 32-bit dropper detects a 64-bit architecture, it drops the 64-bit version. This component drops the Wiper and the Reporter onto the infected computer and executes itself. It spreads across a local network by copying itself to network shares and onto other computers.

The Wiper component utilizes an Eldos-produced driver known as RawDisk to achieve direct user-mode access to a hard drive without using Windows APIs. It identifies the locations of all files on the infected computers and erases them. It sends information about the files destroyed to the attacker and then overwrites the erased files with corrupted data so they cannot be recovered. The component used portions of an image. In the 2012 attack, it used an image of a burning U.S. flag; in the 2016 attack, it used a photo of the body of Alan Kurdi.

Damage caused

The attack unleashed a computer virus to initiate what is regarded as among the most destructive acts of computer sabotage on a company to date. The attack on 35,000 Aramco computers rendered infected computers unusable, causing the company to spend a week restoring its services.

Post Hostilities

Five months later, with a newly secured computer network and an expanded cyber security team, Saudi Aramco brought its system back online. An attack of that size would have easily bankrupted a smaller corporation.

Personal Opinion

The Shamoon attack on Saudi Aramco and RasGas was done by an anti-oppression hacker group. The US attributed Iran as the state sponsor of the attack. This attack can also be seenas a part of the ongoing Middle Eastern Cold war due to religious conflicts between Iran and Saudi Arabia. It can be observed that this attack is an example of how cold war conflicts can transition into a cyber war between the two belligerents.

Sony Corporation Attack 2014

On November 24, 2014, a hacker group identifying itself as "Guardians of Peace" leaked a release of confidential data from the film studio Sony Pictures Entertainment (SPE). The data included personal information about Sony Pictures employees and their families, emails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, plans for future Sony films, scripts for certain films, and other information. The perpetrators then employed a variant of the Shamoon wiper malware to erase Sony's computer infrastructure.

Dispute background

Although hostility between the two countries remains largely a product of Cold War politics, there were earlier conflicts and animosity between the U.S. and Korea. In the mid-19th century, Korea closed its border to Western trade. Korea and the U.S. ultimately established trade relations in 1882. Sony Pictures Entertainment was the victim of a devastating cyber-attack which has been confirmed by US officials that North Korea orchestrated the hack because the North Koreans did not like an upcoming film called ‘The Interview’ by Sony Pictures.

Modus operandi

The malware used in the Sony attack took full advantage of the unprotected files and servers. For example, a hacker could easily spot files named “password”. The breach spread across servers as passwords were freely available to the hackers. The attack was conducted using malware. Although Sony was not specifically mentioned in its advisory, US-CERT said that attackers used a Server Message Block (SMB), Worm Tool, to conduct attacks against a major entertainment company. Components of the attack included a listening implant, backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool. The components clearly suggest an intent to gain repeated entry, extract information, and be destructive, as well as remove evidence of the attack.

Damage caused

According to a notice letter dated December 8, 2014, from SPE to its employees, SPE learned on December 1, 2014, that personally identifiable information about employees and their dependents may have been obtained by unauthorized individuals as a result of a "brazen cyber-attack", including names, addresses, Social Security numbers, and financial information. On December 7, 2014, C-SPAN reported that the hackers stole 47,000 unique Social Security numbers from the SPE computer network.

Although personal data may have been stolen, early news reports focused mainly on celebrity gossip and embarrassing details about Hollywood and film industry business affairs gleaned by the media from electronic files, including private email messages.

Post Hostilities

No clear trail on the source of the attack. Initial reports claimed that there was some Korean language signature in the analysis of the malware. Post attack there was another breach that reportedly pointed to the involvement of Russian hackers.

Accusations had been made against North Korea and others, but ultimately the person(s) responsible for the breach was never brought to justice.

Personal Opinion

The Sony Corporation Attack was carried out by attackers from North Korea in protest against the new movie being released by Sony called The Interview. They found the movie to be disrespectful towards the Supreme Leader of North Korea, Kim Jong Un. Further, relations between North Korea and the United States have been historically tense and hostile, as both countries have no diplomatic relations. This act of cyber warfare was again an act of political respect and agenda.

Wannacry

The WannaCry ransomware attack was a worldwide cyber-attack by the WannaCry ransomware crypto-worm, which targets computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin crypto currency.

Dispute background

Although hostility between the two countries remains largely a product of Cold War politics, there were earlier conflicts and animosity between the U.S. and Korea. Cybercriminals are often state-sponsored and execute actions with tremendous resources leading to a larger impact of the attack. State-sponsored cyber-attacks can have deadly consequences. Linguistic analysis of the ransom notes indicated the authors were likely fluent in Chinese and proficientin English, as the versions of the notes in those languages were probably human-writtenwhile the rest seemed to be machine-translated. According to an analysis by the FBI's Cyber Behavioral Analysis Center, the computer that created the ransomware language files had Hangul language fonts installed. Metadata in the language files also indicated that the computers that created the ransomware were set to UTC+09:00, which is used in Korea.

Modus Operandi

Before ransomware can encrypt files, it needs to locate file shares on the network, which requires performing internal reconnaissance. WannaCry’s behaviors were reconnaissance and lateral movement on the internal network, within the enterprise perimeter. WannaCry spread across local networks and the Internet to systems that have not been updated with recent security updates, to directly infect any exposed systems. To do so it used the EternalBlue exploit developed by the U.S. National Security Agency (NSA), which was released by “The Shadow Brokers” two months before. When executed, the WannaCry malware first checks the kill switch domain name; if it is not found, then the ransomware encrypts the computer's data, then attempts to exploit the SMB vulnerability to spread out to random computers onthe Internet, and laterally to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that their files have been encrypted, and demands a payment of around US$300 in bitcoin within three days, orUS$600 within seven days, warning that "you have not so enough time. " Three hardcoded bitcoin addresses, or wallets, are used to receive the payments of victims. As with all such wallets, their transactions and balances are publicly accessible even though the cryptocurrency wallet owners remain unknown.

Damage caused

The ransomware campaign was unprecedented in scale according to Europol, which estimates that around 200,000 computers were infected across 150 countries. According to Kaspersky Lab, the four most affected countries were Russia, Ukraine, India, and Taiwan.

One of the largest agencies struck by the attack was the National Health Service hospitals in England and Scotland, and up to 70,000 devices – including computers, MRI scanners, blood-storage refrigerators, and theatre equipment – may have been affected. On 12 May, some NHS services had to turn away non-critical emergencies, and some ambulances were diverted.

According to cyber-risk-modeling firm Cyence, economic losses from the cyber attack could reach up to US$4 billion, with other groups estimating the losses to be in the hundreds of millions.

Post hostilities

The attack began at 07:44 UTC on 12 May 2017 and was halted a few hours later at 15:03UTC by the registration of a kill switch discovered by Marcus Hutchins. The kill switch prevented already infected computers from being encrypted or further spreading WannaCry. Experts quickly advised affected users against paying the ransom due to no reports of people getting their data back after payment and as high revenues would encourage more of such campaigns. As of 14 June 2017, after the attack had subsided, a total of 327 payments totaling US$130,634.77 (51.62396539 XBT) had been transferred.

The day after the initial attack in May, Microsoft released out-of-band security updates for end-of-life products Windows XP, Windows Server 2003, and Windows 8; these patches had been created in February of that year following a tip-off about the vulnerability in January of that year. Organizations were advised to patch Windows and plug the vulnerability in order to protect themselves from cyber-attacks.

Personal Opinion

The Wannacry attack was the largest ransomware attack seen by the world. It affected many countries disrupting banking services and businesses around the world. The US attributed this attack to a state-backed hacker group from North Korea. This hacker group was believed to be the same group behind the Sony Corporation attack. The purpose of this attack was to exploit a software vulnerability and earn ransomware but according to reports, it was supported by the government of the country and the actual purpose was to disrupt services and cause unrest among citizens of enemy nations.

US Elections Cyberattack

The Russian government interfered in the 2016 U.S. presidential election with the goals of harming the campaign of Hillary Clinton, boosting the candidacy of Donald Trump, and increasing political and social discord in the United States. According to the U.S. intelligence community, the operation—code-named Project Lakhta—was ordered directly by Russian president Vladimir Putin.

Dispute background

After the break-up of the Soviet Union in 1991 and the end of the Cold War, the U.S.-Russian relationship took on a new dimension, and contacts between citizens expanded rapidly in number and diversity. Not surprisingly, there remain issues on which both governments donot agree. Even after 200 years, the relations continue to evolve in both expected andunexpected ways.

The U.S. intelligence community, in a joint January 6, 2017, declassified report, stated that Russian President Vladimir Putin "most likely wanted to discredit Secretary Hillary Clinton because he has publicly blamed her since 2011 for inciting mass protests against his regime inlate 2011 and early 2012 and because he holds a grudge for comments he almost certainlysaw as disparaging him." On March 20, 2017, FBI Director James Comey testified that Putin "hated Secretary Clinton so much that the flip side of that coin was he had a clear preference.

Modus Operandi

The first method of Russian interference used by the Internet Research Agency (IRA), a Kremlin-linked troll farm, was to wage a social media campaign that favored presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton. The Internet Research Agency also sought to provoke and amplify political and social discord in the United States. Russian use of social media to disseminate propaganda content was very broad. Facebook and Twitter were used, but also Reddit, Tumblr, Pinterest, Medium, YouTube, Vine, and Google+ (among other sites). Instagram was by far the most usedplatform and one that largely remained out of the public eye until late 2018.

The second method of Russian interference saw the Russian intelligence service, the GRU, hacking into email accounts owned by volunteers and employees of the Clinton presidential campaign, including that of campaign chairman John Podesta, and also hacking into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC). As a result, the GRU obtained hundreds of thousands of hacked documents, and the GRU proceeded by arranging releases of damaging hacked material via the WikiLeaks organization and also GRU's personas "DCLeaks" and "Guccifer 2.0".

Damage caused

Advertisements bought by Russian operatives for the Facebook social media site are estimated to have reached 10 million users. But many more Facebook users were contacted by accounts created by Russian actors. Facebook originally denied that fake news on its platform had influenced the election and had insisted it was unaware of any Russian-financedadvertisements but later admitted that about 126 million Americans may have seen posts published by Russia-based operatives.

The Russian military intelligence agency GRU sent "spearphishing" emails that targeted more than 300 individuals affiliated with the Democratic Party or the Clinton campaign, according to the Special Counsel's July 13, 2018 Indictment. Using malware to explore the computer networks of the DNC and DCCC, they harvested tens of thousands of emails and attachmentsand deleted computer logs and files to obscure evidence of their activities. These were saved and released in stages to the public during the three months before the 2016 election. Some were released strategically to distract the public from media events that were either beneficial to the Clinton campaign or harmful to Trump's.

Post hostilities

The question of whether Donald Trump won the 2016 election because of the Russian interference had not been given much focus—being declared impossible to determine, or ignored in favor of other factors that led to Trump's victory. The DNC attack was widely publicized, and documents/emails/other information leaked out to the public via WikiLeaks. Overall, the mission of the adversary was accomplished assuming the original intent was to prevent the DNC candidate from winning the 2016 election.

Personal Opinion

Russia and the United States maintain one of the most important, critical, and strategic foreign relations in the world. There has been fierce competition between the countries in various sectors such as nuclear and space exploration. These espionage and social engineering attacks were clearly orchestrated in order to disturb the political environment in the US. Vladimir Putin was not in the favor of Hilary Clinton coming to power and these preferences though personal at some level, were also highly driven by political agendas. There is also a lot of speculation that Donald Trump coming to power was also due to Russia's interference which displays how cyber attacks have been used to influence cross-border politics.

Analysis of the case studies

Based on the case studies discussed above, we arrive at the following key points related to cyber-warfare.

Evolution of warfare

Human history is filled with warfare between tribes, nations, and empires. The equipment used in war has progressed from sharpened sticks and rocks to automatic guns and predator missiles to today's cyber warfare. Each new piece of military technology changes the way people fight and the tactics employed.

The last major war witnessed by the world was termed World War II. The conflict involved virtually every part of the world during the years 1939–45. By the time WWII started, airplanes had advanced significantly. Since bombers could destroy cities, hit strategic locations, and cause havoc, air superiority became a key factor in the battle plans on both sides. World War II changed the political alignment and social structure of the globe.

Cyberspace, a unique man-made construct, has given a new meaning to war as anyone can attack almost everyone from anywhere at any time. Owing to its virtual nature, the threat landscape has expanded immeasurably, where security concerns engender from faceless and indistinguishable adversaries. Digital technologies have also accelerated the rise of non-state actors as significant entities in world politics.

The United States, along with many other developed nations, has become so dependent on technology that we have become vulnerable to cyberattacks, which can be even more destructive than "traditional" war. The independent conflicts of the Cold War and the drawn-out battles on the field have transitioned into cyber-battles occurring on smaller, less physical scales. Although the US has yet to fight a World War on its own land, a massive cyberattack might have an even greater impact, enabling foreign governments to bring down entire military bases and government headquarters without ever stepping foot into the states. Recent cyberattacks over the past few years indicate a clear movement toward cyber warfare,where government bodies work with hackers to bring down critical infrastructure in other countries. As cybersecurity becomes a top priority for both private companies andgovernment agencies, we should be aware of just how big of a threat hackers pose to ourworld today and tomorrow.

Defense against cyberwarfare

With the growing threat of cyberwarfare, countries and their organizations are looking for ways to dodge the threat entirely or have some fail-safes along the way which allow them to hold their position in case of a cyberattack. The asymmetric nature of cyber-attacks makes defense difficult but an organization, can't afford to leave data security up to chance. This means that in addition to implementing strict cybersecurity policies, organizations should also have to take proactive measures to reduce their cybersecurity risks.

Encryption and Data backup

All sensitive data should be encrypted. Saving data in normal-text format only makes it easy for hackers to access. Data encryption, on the other hand, limits data access to parties that have the encryption key. It also ensures that even when unauthorized parties gain access tothe data, they can't read it.

Regular backups for important information should be conducted. Sometimes cybersecurity breaches can result in data loss. In such a scenario, not having a reliable and secure backup, could result in operational disruptions that could cause an organization a lot of lost revenue.

Regular employee training

Malicious hackers can gain access to your database through phishing emails sent to your employees. These emails contain malicious malware in the form of links that give hackers access to user data, including login credentials. Without proper training, the employee may end up divulging personal information. This is why it's vital that cybersecurity awareness training be conducted. Employees should know the primary forms of cybersecurity attacks and the best ways to prevent them.

Updated system and software

Software and system update highly impact cyber security and digital safety. This is because updates not only add new features but also fix bugs and help patch security flaws and vulnerabilities that can be exploited.

Therefore, a patch management system should be deployed that automatically manages all updates and upholds information security.

A robust cybersecurity policy

An organization's cybersecurity is highly influenced by the policies that they have in place. A thorough cybersecurity policy should have considered the following guidelines-

- **Disaster recovery**: If a breach occurs, a disaster recovery plan ensures that employees and IT teams know the next course of action. It's aimed at reducing the amount of time that you are offline, thereby ensuring that your operations resume as soon as possible.

- **Access control/management**: This policy highlights the parties that can access sensitive information, reducing the risk of unauthorized access. Data mishandling has both financial and legal consequences.

- **Security testing**: This policy should state the frequency of cybersecurity tests conducted in the organization. This allows uncovering vulnerabilities before it’s too late. Some of the security tests that should be conducted include; vulnerability scanning, security posture assessment, penetration testing, ethical hacking, cybersecurity assessments, etc.

COMPARISON

The 21st century has seen a spectacular rise in cyber capabilities. In just over three decades since the World Wide Web entered human lives, now there are more than four billion active internet users with cyberspace penetrating every walk of our lives. Cyberspace has not only subverted political boundaries but also shaken the roots of the system that gave precedence to states. The absence of geographical borders and the apparent opacity in this fifth domain of warfare have allowed a surfeit of malicious non-state actors to come up as security threats.

The advent of cyberwarfare will create various critical changes in the way countries and organizations perceive cyberspace. As more and more countries will adopt cyber warfare the number of cyber-attacks is bound to increase. In addition to this, the anonymity that is considered one of the pros of cyber attacks will create an atmosphere of extreme distrust among countries. Countries A and B with a history of conflict will readily blame each other in cases of such attacks. While another country C might use these opportunities to further its agendas which can cause a shift in political alliances of the world.

The increased unrest and the mistrust among countries can lead to international sanctions from them against states or organizations they see as culprits. These decisions will be made to protect national security interests and defend against threats to international peace and security. Economic and diplomatic sanctions can hamper trade and revenue. Countries might start rejecting electronic parts manufactured in nations with a tainted reputation for orchestrating cyber attacks. These practices will further wane trade and bring in a climate of economic downfall.

As governments turn hostile towards each other we may observe restrictions on travel. Ban on certain electronic items can be foreseen and compulsory information regulations that must be followed to travel to a certain country might be put in place. Some countries might standardize scanning through personal or professional devices leaving the country to restrict any data sensitive to national security. These practices will cause concerns about the privacy of traveling individuals. Restrictions such as these will act as a deterrent to international travel and relations.

Restrictions on travel and the decline in trade will cause isolation between countries. Countries will seek to be independent. This scenario will cause various multinational corporations to suffer. These security policies might cause the MNCs to pull out their resources from that country. The workforce of an MNC might also take decline due to the decrease in the number of countries allowing a corporation to operate in their jurisdiction.

Following all this, governments of the world might decide to bring laws and regulations governing cyberspace. These laws would act to limit world governments from using cyberspace as a means to disrupt other nations. It will execute regulations allowing governments and organizations to only collect certain data and ensure privacy as well as security of the citizens of the world. Considering the existing Treaty on Prohibition of Nuclear Weapons put in place to ensure a nuclear fallout doesn’t occur, a similar treaty to eliminate the threat of cyber warfare will be also needed to be put into action.

All these changes might be observed in the near future as more and more countries move towards conquering cyberspace and aim to become the governing political power of the world. The perplex modus operandi of non-state actors, their unusual anatomy, confusing allegiances, and diverse motivations will drastically affect strategy in the cyber world and make extenuating their impact onerous.

CONCLUSION

The objective of this research paper was to analyze historical cases of cyber-warfare and understand cyber-warfare. It was observed how disputes between countries led to the sanctions for cyber attacks. We learned the various approaches taken by different governments to orchestrate such an attack. Further, we looked into the strategies that should be put in place by various current governments of the world to try and shield themselves from such an attack. Lastly, we saw how the advent of cyber warfare is bound to change the world in years to come, forcing governing agencies of the world to come up with laws or a single autonomous body to stop cyber warfare.

We hypothesized how the evolution of cyber warfare as an effective and preferred mode of war will have a momentous impact on the ever-changing structure of political power in the world. It was seen that the pace of innovation in the cyber sphere has been greater than in any other domain of warfare. Cyberattacks, without causing direct injury to humans, have ensured harm to physical infrastructure worth billions, which eventually affect human lives. Taken in the context of geopolitics, a digital weapon like Stuxnet could simply be understood as the most expedient, non-violent, and cost-efficient method to covertly disrupt a nuclear weapons program. At least, this is how politicians would see it — when contrasted with traditional war-making tools, such as fighter jets, soldiers, or bombs.

Two centuries ago, military historian Carl von Clausewitz said that "War is the continuation of Politics by other means". In today’s scenario, cyber war seems to be the weapon of choice for some, a continuation of politics in other means. This present will lead to a future where cyber attacks will hold the power to shift political alliances of the world

Future Work

The research paper does not take into account the various cyber policies that nations and organizations are coming up with at present. We need to consider what kind of restrictions will these laws pose on the governments of the world. These regulations will further decide how cyber warfare develops in the future. Cyberspace might convert into a safe space after all the world governments decide to regulate it.

The scope of these laws and regulations is vast and can be included to further the research on this topic.

BIBLIOGRAPHY

Anon, 10 ways to reduce cybersecurity risk for your organization. *Upguard*. Available at: https://www.upguard.com/blog/reduce-cybersecurity-risk [Accessed September 22, 2022].

Anon, 2021. What is cyber warfare: Types, examples & mitigation: Imperva. *Learning Center*. Available at :https://www.imperva.com/learn/application-security/cyber-warfare/[AccessedSeptember 22, 2022].

Anon, 2022. Iran–Saudi Arabia proxy conflict. *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Iran%E2%80%93Saudi_Arabia_proxy_conflict [Accessed September 22, 2022].

Anon, 2022. Russian interference in the 2016 United States elections. *Wikipedia*. Available at: https://simple.wikipedia.org/wiki/Russian_interference_in_the_2016_United_States_ele ctions [Accessed September 22, 2022].

Anon, 2022. Secondary research: Definition, methods, & examples. *Qualtrics AU*.Available at: https://www.qualtrics.com/au/experiencemanagement/research/secondaryresearch/?rid=ip&prevsite=en&newsite=au&geo=IN&geomatch=au [Accessed September 22,2022].

Anon, 2022. Shamoon. *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Shamoon [Accessed September 22, 2022].

Anon, 2022. Sony Pictures hack. *Wikipedia*.Available at: https://en.wikipedia.org/wiki/Sony_Pictures_hack [Accessed September 22, 2022].

Anon, 2022. Stuxnet. *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Stuxnet[Accessed September 22, 2022].

Anon, 2022. WannaCry ransomware attack. *Wikipedia*. Available at: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack [Accessed September 22, 2022].

Anon, What is cyber warfare? *Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/cyber-warfare#:~:text=Cyber%20Warfare%20is%20typically%20defined,denial%2Dof%2Dservice%20attacks [Accessed September 22, 2022].

Djs, 2021. Pros and cons of cyber warfare. *Bohatala*. Available at: https://bohatala.com/pros-cons-cyber-warfare/ [Accessed September 22, 2022].

Elazari, K., 2021. Cyber warfare in global conflicts. *Iberdrola*. Available at: https://www.iberdrola.com/shapes-en/keren-elazari-cyber-warfare-in-context-of-global-conflicts [Accessed September 22, 2022].

Gazula, M.B., 2017. Cyber Warfare Conflict Analysis and Case Studies. *MIT CAMS*. Available at: https://cams.mit.edu/wp-content/uploads/2017-10.pdf [Accessed September 22, 2022].

Menon, N., 2021. The potential impact of cyber capabilities on future strategy. *E-IR*. Available at: https://www.e-ir.info/2021/05/05/the-potential-impact-of-cyber-capabilities-on-future-strategy/ [Accessed September 22, 2022].

O'Neil, M., 2016. Cybercrime dilemma: Is it possible to guarantee both security and privacy? *Brookings*. Available at:https://www.brookings.edu/articles/cybercrime-dilemma-is-it-possible-to-guarantee-both-security-and-privacy/ [Accessed September 22, 2022].