CYBERWARFARE

Archita Srivastava*

INTRODUCTION

When someone mentions the word 'war,' the image that pops up in one's mind is naturally that of an army of soldiers in a battleground with a gun in their hand. However, this is not the only kind of warfare to exist. Over the years, different types of mechanisms have been employed to express the tension between two nations- Cold War, nuclear war, etc. As a result, there are multiple kinds of warfare that are used by countries in the current scenario, cyber warfare being one of them.

The internet is no longer just a place where people have access to videos and news articles, but it has emerged as a forum where sensitive personal data is being shared as well. In a world where AI is developing and being used at an extremely fast pace, due to which there is an increasing reliance on digital networks, it is no shocker that this same tool can soon end up being a threat to an entire nation at large, especially in times of war.

WHAT IS CYBERWARFARE?

Although experts are still not clear as to what exactly qualifies as cyberwarfare, and there are many debates making rounds for the same, cyber warfare, as has been defined by the Oxford Dictionary, is the use of computer technology to disrupt the activities of a state or organisation, especially the deliberate attacking of information systems for strategic or military purposes.[1] This attack can be perpetrated by a nation, a terror organisation or even non-state actors pursuing a hostile nation's aim.

Since cyberwarfare concerns sensitive information that can affect a nation at large, it can cause significant damage. The main purpose behind the usage of cyber warfare is to give one nation the upper hand over another, since it has the potential to wreak havoc on government and

*BA LLB, FIRST YEAR, GOVERNMENT LAW COLLEGE, MUMBAI.
[1] Oxford Dictionary

civilian infrastructure and disrupt critical systems, resulting in damage to the state and even loss of life.[2]

DIFFERENCE BETWEEN CYBERCRIME AND CYBERWARFARE

Usually, people consider cybercrime and cyberwarfare to be the same. However, that is far from the truth. Cyberwarfare is a type of cybercrime. Thus, all situations of cyberwarfare amount to cybercrimes, but all cybercrimes do not amount to cyberwarfare. The main difference between the two lies in the intensity of the attack. Cybercrimes are usually those offences that are committed against individuals or a group of individuals, with a malicious intention to tarnish the reputation of the individual/s directly or indirectly, using cyberspace. Cyberwarfare, on the other hand, concerns the safety of a nation at large. It is an internet-based conflict involving politically motivated attacks on the information system of another country, which can further cripple the social base of the country. It also proves to be favourable for the country perpetrating the attack, as they are supplied with sensitive data like healthcare records, bank details, etc. To sum it up, while cyberattacks are usually executed on a smaller scale, cyber warfare is always executed on a larger scale, thereby making it a bigger threat to society.[3]

TYPES OF CYBERWARFARE

Cyber Espionage: Since espionage is synonymous with the word 'spying,' this type of cyber warfare is also referred to as cyber spying. It essentially involves the use of computer networks to gain illicit access to confidential information that is typically held by the government. In other words, computer systems are hacked to gain access to sensitive information. This is carried out using techniques like botnets or spear phishing, both of which infiltrate into the system under the guise of trustworthy individuals, devices, links, etc.

Cyber Sabotage: Countries or organisations attack computer systems in order to disrupt online services and gain access to sensitive information, thereby enabling them to gain a strategic advance on the global front. When cybercriminals are responsible for the same, they usually demand a ransom in return for access to the services they have hacked. The sensitive

[2] Anonymous, 'What is Cyber Warfare' (imperva) <**What is Cyber Warfare | Types, Examples & Mitigation | Imperva**> accessed 22 September 2023

[3] Cheistha, 'Differentiate between Cybercrime and Cyberwarfare' (INSIGHTSIAS, 24 December 2014) <9) Differentiate between cybercrime and cyberwarfare. It is said that cyberattackers have more advantages over agencies fighting cyberthreats. Examine these advantages - INSIGHTSIAS (insightsonindia.com)> accessed 22 September 2023

information accessed in this scenario is generally certain assets and critical infrastructures, thereby impacting various kinds of activities ranging from those that are performed daily to those that are crucial for the safety and security of the nation.[4] As a result, this destabilizes the nation under attack. A more specific type of warfare under this category is the denial-of-service (DoS) attack, which renders networks inaccessible to users or the rollout of other malware intended to disable computer systems.[4]

Propaganda Attack: The cyber and digital space plays a crucial role in swaying the opinion and perception of the people, especially in the status quo. Propaganda attacks refer to those attacks which expose uncomfortable truths or spread lies to deceive the public, and sow a feeling of distrust and dissent for the government among the people, thereby inducing an atmosphere of disharmony as well as unrest. This tool is used to influence the minds of the people belonging to that nation. As a result, it also falls within the realm of psychological warfare.

The rising prevalence of Artificial Intelligence has led to a fear of deepfakes as well. Deepfake refers to a video of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information.[5] Since establishing the truth or falsity of the video is quite difficult on a surface level, this can be used for political propaganda to create unrest among the citizens, which can further lead to riots. To add on, this can make a nation vulnerable to external threats as well.

Economic Disruption: This method mainly deals with attackers targeting the network system of banks, payment systems and stock markets with the purpose of stealing money or blocking others from gaining access to their funds.[1] Thus, this weakens the economic level of a nation by systematically destroying the soft power of that nation. Further, this can lead to many devastating side effects, such as the country being unable to afford basic necessities, shortage of equipment for the army, and so on. Consequently, the targeted nation is handicapped in terms of its resources.

Electric Power Grid Attacks: This kind of cyber-attack is focused on disabling a country's power grid, by damaging power lines or generators, and consequently sabotaging physical infrastructure. It can also be carried out digitally by hacking into the computer systems that

[4] Haroun Alfarsi, 'Different Types of Cyberwarfare' (Profulus, 23 March 2022) <https://www.profolus.com/topics/different-types-of-cyberwarfare/> accessed on 22 September 2023
[5] Oxford Dictionary

control the power grid and causing them to malfunction. Power grid attacks have terrible repercussions, as they can cause widespread blackouts, economic damage, and even the death of people.

GOALS OF CYBER WARFARE

The primary goals of cyberwarfare are:

- Disrupting, damaging, or destroying a country's computer networks and infrastructure. This goal is usually achieved by carrying out digital attacks that disable critical systems or render them unusable. This can include targeted cyberwar attacks on power grids, financial systems, transportation networks, and communication networks.[6]
- Stealing sensitive information or causing economic damage. The goal is achieved by stealing data or money or causing economic damage through the destruction of property or the loss of business.

HISTORY AND OCCURRENCES

Bronze Soldier (2007): When the Estonian government moved the Bronze Soldier, a painful symbol of Soviet oppression, from the capital of Estonia to a military cemetery on the outskirts of the city, the country was attacked several times through cyberwarfare. As a result, numerous banks, media outlets as well and government sites were taken offline due to unprecedented levels of traffic.

The Stuxnet Worm (2010): The Stuxnet Worm, which is still considered to be one of the most sophisticated malware attacks in history, was used to attack Iran's nuclear programme. Designed by the United States of America and Israeli intelligence, under the classified programme 'Operation Olympic Games,' it targeted Iranian supervisory control and data acquisition systems, intending to derail or at least delay the nuclear mission, by destroying the centrifuges that were being used to enrich Uranium, as part of the programme.[7]

Distributed Denial of Service Attack in Ukraine (2014: It was reported that the Russian government had allegedly initiated a Distribution Denial of Service Attack against Ukraine,

[6] Taras T, 'The First Cyberwar is Now; What is Cyberwar?' (Geniusee, 4 April 2022) <The First Cyberwar Is Now; What Is Cyberwar? | Geniusee> accessed on 22 September 2023
[7] Josh Fruhlinger, 'Stuxnet Explained: The First Known Cyberweapon' (CSO, 31 August 2022) <Stuxnet explained: The first known cyberweapon | CSO Online> accessed on 22 September 2023

that the Russian government allegedly perpetrated a DDoS attack that disrupted the internet in Ukraine, enabling pro-Russian rebels to take control of Crimea.

Sony Pictures (2014): Upon the release of the movie 'The Interview,' which portrayed the North Korean leader in a bad light, hackers associated with the government, were said to have carried out a cyberattack on Sony Pictures. The FBI investigated the issue and found that the pattern of the data contained in the malware used was similar to data accessed through previous cyber-attacks by North Korean hackers. This included encryption algorithms, data deletion methods and compromised networks.

The U.S. Presidential Election (2016): The "Report on the Investigation into Russian Interference in the 2016 Presidential Election" by Special Counsel Robert Mueller established that Russia used the tool of informational warfare in order to interfere with the U.S. presidential election. This was done with the help of social media accounts and interest groups It developed from being an operation that discredited the electoral system in 2014 to engaging in activities designed to benefit candidate Donald Trump in the 2016 election.[8] Thus, it served the purpose of messing with the minds of the voters and shaping their political views and opinions, thereby making it a propaganda attack.

China's Ministry of State Security (2018): Two Chinese hackers, associated with the Chinese government's Ministry of State Security, were accused of targeting intellectual property and confidential business information. This act had the potential to not only harm America's economy by targeting their businesses and consumers but also give unfair leverage to China on the global platform. Their main aim was to commit computer intrusions, wire fraud and even aggravated identity theft. The indictment further alleged that the defendants were associated with a group that had hacked computers in at least a dozen countries and provided the intelligence service of China with access to sensitive business information.[9]

Iranian weapons systems (2019): As a retaliation for the shooting of a US drone by Iran, the US launched a cyberattack against Iranian weapon systems. This in turn disabled the computer systems responsible for controlling the rocket and missile launchers.

[8] Alexander S Gills 'Cyberwarfare' (TechTarget, March 2023) < What is Cyberwarfare? | Definition from TechTarget > accessed on 22 September 2023

[9] Office of Public Affairs | Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information | United States Department of Justice

Pegasus Spyware (2021): Pegasus Spyware, developed by an Israeli cyber arms company 'NSO Group,' was designed in a manner to enable it to be covertly installed on certain mobile phones. Although it was portrayed as a product meant to fight terrorism, governments around the world have occasionally used the same product to keep a check on journalists, human rights activists, lawyers and so on.[10]

The most surprising feature of this spyware is that it follows the zero-click method, unlike most other spyware. This feature enables the spyware to infect even those devices whose owners have not clicked on any seemingly trustworthy link or mail. Even in cases wherein the user deletes the message, upon finding it suspicious, the spyware still manages to get installed, making it very difficult for the targeted individuals to protect themselves.[10]

Ukraine and Russia (2022): Ukraine witnessed a significant increase in cyber-attacks during their war against Russia, which were led by well-known groups. Malware, data wipers, DDoS attacks, etc, meant to target critical industrial infrastructure, data networks, and public and private sector organizations were used in the attacks. The primary aim of the attacks has also changed over the course of the war, from destruction of critical infrastructure to information and intelligence gathering.[7] This was not the first time Russia has implemented the use of cyber warfare against Ukraine, as the nation has also been associated with electric power grid attacks, cyber espionage and cyber sabotage. In fact, Russia has also been accused of weakening the Ukranian artillery. Thus, over the years, cyberspace has been actively used as a medium to weaken other countries and gain an upper hand, especially during times of war.

AIIMS Ransomware Attack (2022): All India Institute of Medical Sciences (AIIMS), a prestigious hospital that also deals with high-profile cases, was hit by a ransomware attack in the year 2022. This risked sensitive data of health records of important politicians from being leaked, which could have further threatened the security of the country. This attack also interfered with the daily operations at the hospital- appointments, patient registration, and discharge and so on. As a result, this attack slowed down the working of the hospital and led to a dicey situation, wherein the health record of millions of Indians, including important politicians, leaders and public figures, was at risk.

[10] Madhur, 'What is Pegasus Spyware and How It Works?' (GeeksforGeeks, 2 August 2021) <What is Pegasus Spyware and How It Works? - GeeksforGeeks> accessed on 22 September 2023

LEGAL FRAMEWORK

With a steady advance in the field of Artificial Intelligence and Technology, there is an increasing need for stringent laws and regulations to curb the use of cyber warfare as much as possible. However, a lack of clarity regarding the exact regime of cyberwarfare makes this task difficult. As a result, the legal status of this matter is still unclear, since there is no international law that governs the use of cyber warfare yet. To add on, as and when the laws are passed, it is essential for the laws to be up to date with the cybercrime cases occurring across the globe. [11]

HOW TO COMBAT THIS ISSUE

Since the current legal framework does not deal with how to curb the use of cyber warfare, it is even more essential for countries to take certain steps to be able to combat this issue, or at least assess how strong their defense is. The following methodologies can be implemented:

- Conducting risk assessments with cyberwar games, which will act as a real-life exercise or simulation. The above technique will help test a nation's readiness to be able to overcome threats of cyberwarfare.[5]
- Many governments have adopted operational national security strategies to protect their information infrastructure in the face of cyberwarfare, which will further help strengthen their defence on the cyber front.[5] Other countries must also take a step in this direction, as it has the potential to decrease the possibility of a successful cyberattack against their nation.
- Antivirus software must be used on a large scale. This software must be updated enough to be able to combat the developing means and mechanisms to penetrate into the cyberspace of a country.

CONCLUSION

It is a well-known fact that in the past few years, the world has come a long way in the field of technology and artificial intelligence. To add on, despite the first incident of cyber warfare dating back more than 15 years ago, no real progress has been made regarding laws dealing with cyber warfare. As a result, there is a huge possibility for the occurrence of cyber warfare to significantly boost in the coming years, especially because of the increasing dependence on

[11] Sakshi Shairwal, 'Legal Understanding of Cyberwarfare in India' (Lexology, 24 January 2022) < Legal understanding of cyber warfare in India - Lexology > accessed on 22 September 2023

technology. The Russia-Ukraine war is the best evidence to support this assertion, wherein cyberspace was used as a weapon throughout the course of the war. There have been several occurrences in the past few years wherein the cyberspace of one country was penetrated into and then destroyed. This was done using the various mechanisms of executing cyber warfare. The constant use of cyber warfare should serve as a warning to all the nations and organisations across the globe, and allow them to foresee what lack of laws dealing with cyber warfare can cause, as it does not only imply penetration into cyberspace but also the destruction of power grids, interference in daily affairs, hindrance in communication and many more dangerous consequences.