INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

EMERGING THREATS AND LEGAL RESPONSES OF CYBER WARFARE

AUTHORED BY - SIMAR KAUR CHAWLA

Abstract

The emergence of cyberwarfare has completely changed the way war is fought, raising doubts on the traditional views about international law and warfare. This research examines the new risks that cyberwarfare poses in the current scenarios. This paper also delves into the legal frameworks controlling cyber operations and evaluates how well they match the difficulty of existing cyberthreats. This study also examines how international organisations and legal frameworks contribute to the improvement of cyber security and stability. This paper also tries to make the people aware about the types of cyber war attacks. The study also analyses the effectiveness of legal actions and defensive measures implemented by countries and the international community to reduce the threats posed by cyber warfare. It also looks at how new developments in artificial intelligence, quantum computing etc will affect the nature of cyberwarfare in the future and the laws that will govern it.

In the end, this research advances our knowledge of the dynamic nature of cyberthreats and the need for strong legal defences to protect national security, respect international law, and maintain the stability of the global cyberspace.

Keywords:

Cyberwarfare, Cyber-attack, Cyber Threats, Cyber Space, Cybersecurity, Cybercriminals

Introduction

Cyber Warfare is a cyber-attack by a foreign country towards any other country or organisation with the aim to disrupt or damage their infrastructure, computer systems or information network with the use of computer viruses, malwares, etc. The main aim for cyber warfare is not financial gain but to weaken the country or the enemy state or any organisation. Since cyber warfare is a series of cyber-attacks, we must know what cyber-attack means. Cyber-attack is the attempt to get unauthorised access to another's computer network with the intention to destroy, damage,

ISSN: 2582-6433

disrupt these networks and also to meddle with and tamper the data stored in these computers or electronic devices. There is no universal or one clear definition of cyber warfare and there is even a debate going on among the cyber security experts as to what cyber-attack constitutes a cyber warfare.[1] The cyber warfare takes place in the cyber space which is virtual world with interconnected computer network systems or electronic mediums which are used for communication, transfer of data, interaction among people from all over the world, sharing ideas, playing games etc. Cyber security is one of the most difficult challenges in cyber space and when this security is not taken care of then this results into cyber-attack and cyber warfare.

Background

The world has evolved a lot with the help of information technology. This information technology has brought people closer to each other irrespective of their geographical boundaries. This has no doubt had a lot of advantages and it has helped many economies in developing but it has also created challenges for cyber security. There have been quite a few instances of cyber warfare and it had a lot of disastrous impacts on the economy and people of the particular country, state or organisation on which the attack was made. The origins of cyber warfare can be traced back to 2010, when *Stuxnet* was the first actual cyberweapon designed to cause physical damage. A worm attacked Iran's nuclear programme. It is one of the most advanced cyber-attacks in history. Malware transmitted through infected USB devices, which targeted data collecting and supervisory control systems. According to most sources, the attack severely harmed Iran's ability to produce nuclear weapons.[2]

This *May 2014, Russia vs. Ukrainian election commission*: Three days before Ukraine's presidential election, a hacking gang based in Russia brought down both the election committee and its backup system. The attack was intended to cause confusion and promote the pro-Russian candidate. June 2015, *Russia vs. German Parliament*: German investigators revealed that hackers had hacked the Bundestag's computer network. The BfV, Germany's domestic intelligence organisation, later stated that the attack was carried out by Russia and said that they were looking for information on the operations of the Bundestag, German politicians, NATO, and other. May 2017, *WannaCry*: This attack is believed to have affected over 200,000 machines in 150

**Ms. Simar Kaur Chawla, Student BBA LLB 3rd year, Bharati Vidyapeeth (Deemed to be University) New Law College, Pune.*
[1] What is Cyberwarfare, TechTarget, (https://www.techtarget.com, last visited-20/1/24,2:00PM)
[2] What is Cyber Warfare/Types, Examples and Mitigation, imperva, (https://www.imperva.com, last visited-21/1/2024,12:35PM)

ISSN: 2582-6433

countries. WannaCry was a type of ransomware cryptoworm that attacked systems running Microsoft Windows. June 2017, NotPetya: This is the first major incidence of weaponized ransomware. The *NotPetya* software was camouflaged as ransomware, but its ultimate objective was to delete files. While the attack began in Ukraine, it swiftly went globally. It is unclear how much damage was caused during this strike, although it is thought that the overall loss exceeded $10 billion USD.[3]

Sony Pictures Hack- Following the theatrical release of movie "The Interview," which depicted Kim Jong Un negatively, an attack was launched against Sony Pictures. The attack is blamed on North Korean government hackers. The FBI discovered commonalities with prior North Korean malware operations, such as code, encryption methods, and data destruction mechanisms.[4]

Cyber Attack on Indian Healthcare Websites - In 2019, cyber-attacks targeted Indian healthcare websites. According to cyber security organisations based in the United States, hackers broke into and infiltrated a major healthcare website in India. The hacker grabbed 68 lakh details of patients and doctors.[5]

The objective of cyberwarfare is to weaken, destroy, and damage another nation. Cybercriminals use a variety of cyberwarfare techniques, including destabilisation, to target nation-state governments by breaking into their systems of banking, transportation, water supply, power supply, hospitals, and other infrastructure. By attacking through infrastructure, they can easily disrupt the working of the nation. These cyberwarfare attacks have various effects. Just as mentioned about the sectors like banking can have serious effect of the cyber attack like there could be a huge financial loss and if the data of the banking companies is stolen then it can cause huge losses to the banking company and it will prove to be a very big problem for the economy. Same way the hackers can also disrupt the transportation system by hacking the technology. This all can lead to delay in transportation facilities provided to the civilians like delay in trains etc.[6]

There has been a significant evolution in the nature of cyber threats over the time period. Cyber-attacks are not just limited to random pop-ups on our screens or fake emails it has evolved a lot

[3] A Brief History of Cyberwarfare, Gra quantam, (https://graquantum.com/a-brief-history-of-cyberwarfare/, last visited-24/1/2024,1:20PM)
[4] Imperva, (https://www.imperva.com,lastvisited,23/1/2024,1:30PM)
[5] Kratikal Blog, (https://kratikal.com/blog/5-biggest-cyber-attacks-in-india/,lastvisited,24/1/2024,1:35PM)
[6]Dhanya Airen, Cyber Warfare And its Impact Legal Service India, (https://www.legalserviceindia.com,last visited-24/1/24,2:10PM)

ISSN: 2582-6433

to data breaches, cloud vulnerabilities, phishing etc. The main reason for these new threats is the fast-developing technology. One of the best examples for this new evolving technology is the AI which has imposed a serious threat on the virtual world and is helping the cyber criminals to launch attacks more easily.

Types of Cyberwarfare attack

Espionage: It involves keeping an eye on other nations in order to obtain secrets. In cyberwarfare, this can mean hacking into computer systems that are vulnerable by using spear phishing or botnets, and then stealing sensitive data. This attack is often considered same as the cyberwarfare but its different as the main aim of cyberwarfare is to disrupt the activities of the nation-state but the main aim of espionage is to stay inside the network system for as long as possible and steal their data by spying on them.[7]

- **Sabotage**: Government organisations must identify sensitive data and the dangers associated with its exploitation. Foreign governments or terrorists may steal information, destroy it, or exploit insider threats such as dissatisfied or negligent personnel, or government workers with ties to the attacking country.
- **Denial-of-service (DoS) Attack**: DoS attacks prohibit actual users from visiting a website by flooding it with false requests, forcing the website to handle them. This form of attack has the potential to interrupt important operations and systems, as well as prevent individuals, military and security professionals, or research organisations from accessing sensitive websites.
- **Propaganda attacks**: These attacks aim to influence the minds of those residing in or fighting for a specific country. Propaganda is commonly used to disclose uncomfortable truths, propagate lies to destroy people's belief in their government, or align with their enemy.[8]
- **Data Theft**- In an attack like this these cybercriminals steal the sensitive data of the individual and hold it for ransom or sell it or they can even destroy these important, sensitive data.

People and organisations can protect themselves from these cyberwarfare attacks. The first thing that needs to be done to prevent from becoming a prey to these attacks is to create awareness among the organisations and the people about the various cyber-attacks that are prevailing in the

[7] supra note 1
[8] supra note 3

ISSN: 2582-6433

cyberspace and how dangerous their impacts can be. People can protect themselves from these attacks by downloading cybersecurity software's which are easily available, protect the data with the help of two-factor verification so that it becomes difficult for the attacker to gain access to your personal data etc. With increasing cyber-attacks there is also evolution of cybersecurity measures and these measures should be used by the individuals to stay protected from these attacks.

Emerging Cyber Threats

New cyber threats are emerging everyday due to the fast-growing technology. Due to these fast-evolving technologies it has become easy for the attackers to exploit the cyber space and these attackers can be anyone be it a state or an individual hacker or even a group. It is very difficult to keep pace with such evolving technology. Some examples of evolving cyber threats are:

- **Advanced Persistent Threat (APT)-** These are cyber-attacks conducted by a single or a group of experienced cyber criminals. The main motive of this type of attack is to get inside the network systems and to steal as much data as possible. This attack is not just to get in and out, during this attack the intruders try to stay in the network as long as possible and after they establish a foothold then they try to gather as much data as possible without getting caught and even try to expand their area. These attacks are sometimes even sponsored by the states. After the intruders have collected enough data, they extract the data from the network without being detected with the help of white noise tactics. These attacks are used as cyberwar weapons.[9]
- **AI-Powered Attacks-** AI is now being used as a cyber security weapon. It has the mechanism to detect cyber-attacks and helps to prevent it. On the other hand, cybercriminals are using this technology to enhance the effectiveness of their attacks. So, on one hand it is helping in preventing cyber threats and on the other creating new ones.
- **Supply Chain Attacks-** This is a type of attack in which the cybercriminals attack the third party that is the supplier of that particular company to get access to the company's data. These attacks can be done on software providers or cloud storage providers etc. These suppliers become an easy source to get unauthorised access to a particular organisations network system and data and so are prone to these attacks.
- **State Sponsored Attacks-** State-sponsored cyberattacks are digital operations carried out or sponsored by national governments for political, economic, or military goals. These

[9] Advanced persistent threat (APT), imperva, (https://www.imperva.com, last visted-25/1/24,4:30PM)

ISSN: 2582-6433

attacks target government organisations, essential infrastructure, military systems, or private businesses. Attribution of state-sponsored attacks is frequently difficult due to the use of proxies, false flag operations, and complex tradecraft. This is also a weapon of cyber warfare.

- **Internet of Things (IoT)-** It is a network of interconnected devices which facilitated communication between the devices. IoT is going to be an essential element in future because these devices do not have a strong security system which is a drawback and which is a loophole for the cybercriminals to attack on these devices for example security cameras. It becomes necessary for the organisations to have a strong security software for these devices which will prevent cyber threats related to these devices that is IoT. They can even use two factor verification for more protection.

Legal Framework

There was an urgent need for special cybersecurity legislation in light of recent technological advancements and emerging cyberthreats. India adheres to the Information Technology Act, 2000, which was revised in 2008 and is currently known as the Information Technology Amendment Act, 2008, as the country lacks specific cybersecurity legislation.

We'll talk about a couple of this act's crimes and its provisions that address cybersecurity and are related to cyberwarfare.

- **S.43- Penalty and compensation for damage to computer, computer system, etc. (Amendment vide ITAA-2008):** This section talks about the provisions regarding unauthorised actions and access relating to computer and computer networks. It prohibits individuals from accessing the computer or its networks without proper permission and also prohibits downloading or extracting information without authorisation. It prohibits the individuals from introducing any virus into the computer system or damage the computer, database or its programs. It also prohibits the individuals from manipulating any data that is deletion or alteration in the information stored in the computer or its system is prohibited. S.66 mentions the punishment to be given to a person who does any act prohibited under section 43 and that he shall be punished with imprisonment for a term which may extend to 2-3 years or with fine which may extend to 5 lakhs rupees or with both.[10]

[10] Section 43 of Information Technology Amendment Act, 2008, No.10 of 2009(India)

ISSN: 2582-6433

Chapter XI of this amendment act is OFFENCES and has some crimes and its provisions related to cyberwarfare:

- **S.66C- Punishment for identity theft:** Anybody found to have used another person's password, electronic signature, or other unique identifying feature dishonestly or fraudulently faces up to three years in prison and a fine of up to one lakh rupees.[11] During cyberwarfare the attackers try to steal the sensitive data from the computer networks which also can be unique identity information or a data base of passwords or digital signatures. The attackers may use this information for identity theft and can be punished under this section.
- **S.65- Tampering with computer source code:** If someone is found to have purposefully concealed, destroyed, altered, or caused another to do so with respect to any computer source code used for a computer, computer programme, computer system, or computer network and the source code is required to be kept or maintained for the duration of the law, they could face up to three years in prison, a fine of up to two lakh rupees, or both.[12]

National Cyber Security Policy, 2013: With the goal of safeguarding India's information infrastructure from online attacks, this strategy establishes a framework for cyberspace security. Although the strategy doesn't specifically define terms that relate to "cyberwarfare" in the traditional sense, but it does establish a number of important objectives and strategies meant to improve India's cybersecurity position. The policy tries to create a secure cyber ecosystem to insure the safety of the cyberspace. To effectively reduce cyberthreats, it involves cooperation between governmental bodies, businesses, academic institutions, and international organizations. This policy also encourages the need for more skill development in the cybersecurity professionals so that they become more capable to prevent the cyber-attacks and cyber threats.

Challenges in enforcing cyber related laws

- **Problems with attribution:** It is frequently difficult to correctly attribute cyberattacks due to the complexity and the involvement of numerous countries in determining the genuine origin and identity of cyber attackers.
- **The cross-border nature of cybercrime:** Cybercriminals can operate from any area with an internet connection, as cybercrime has no geographical bounds. It can be

[11] Section 66C of Information Technology Amendment Act, 2008, No.10 of 2009(India)
[12] Section 65 of Information Technology Amendment Act, 2008, No.10 of 2009(India)

ISSN: 2582-6433

difficult and time-consuming to coordinate investigations and enforcement activities across international borders.

- **Restricted Technical Knowledge:** It's possible that courts and law enforcement organisations lack the resources and technological know-how necessary to adequately investigate and prosecute cybercrimes. Technological complexity is a common tool used by cybercriminals to avoid detection and prosecution.
- **Ambiguity in Jurisdiction:** Due to the international character of cyberspace, there are concerns regarding national laws' applicability to cross-border cyber activity as well as jurisdiction. It can be difficult to establish jurisdiction and decide which laws apply, particularly when there are international individuals involved.
- **Data Privacy Issues:** A major problem lies in creating a balance between need for law enforcement to have access to electronic evidence and people's right to privacy. It is difficult to obtain access to protected data and electronic personal communications for investigation purposes while maintaining privacy rights.

Gaps in the current legal framework

- **Lack of Harmonization:** Legal frameworks relating to cybersecurity and cybercrime are very different in all the countries which leads to inconsistency. Improving cooperation globally and harmonizing legislation are necessary to effectively overcome cross-border cyber threats.
- **Insufficient Cybercrime laws:** Due to the lack of comprehensive cybercrime laws there is a gap which is preventing us to tackle the problem of cybersecurity. There is a need for robust laws to fight against cyber-attacks.
- **Lack of International Cooperation:** International cooperation that is cooperation among various countries is very essential to fight against and to prevent cyber-attacks. The existing international cooperations are insufficient and slow and hinders the coordination among countries.

These are some of the gaps in the current legal framework that needs to be filled which will make the country sufficient in itself to fight against all the cyber threats in future.

ISSN: 2582-6433

Submission

In conclusion, the research paper on emerging threats and legal responses on cyberwarfare has shown how cyberwarfare has changed the notion of warfare and international law. It shows how with evolution of time and technology these technological changes have posed a significant threat to the cyberspace and cybersecurity. Through the analysis of present legal framework, we get both its strength and weakness in tackling the problem of modern cyber warfare. Through this paper we also get the idea about the emerging cyber threats. Anticipating and minimizing the risks associated with future cyber threats is essential as we manage the effects of developing technologies like artificial intelligence, quantum computing, and the Internet of Things. This study emphasises how important strong legal measures are to maintaining cyberspace stability, promoting international coordination, and protecting national security. The evolving nature of cyber threats demand flexibility in adapting with the new challenges both nationally and internationally. From the researcher's point of view, I would like to recommend that a separate and robust legislation should be made for all cyber related matters be it an attack or a war. Its hight time that it is made because with new cyber attacks coming on a regular basis it becomes very difficult to legally deal with them without any proper legislation. Only with a proper legislation will victims of cybercrime be able to get justice.