Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Cybersecurity on the Global Stage: Advocating for a Cyber United Nations like body Cyber-WHO

Hina Iliyas[a]

[a]Assistant Professor, Hidayatullah National Law University, Raipur, India

Received 09 September 2023; *Accepted* 02 October 2023; *Published* 05 October 2023

In today's digital era, the Internet holds a pivotal role in our daily lives, manifesting itself in numerous conspicuous ways. The digital landscape has not only revolutionized our existence but has also ushered in novel modes of communication, organization, and information access. However, this transformation, while empowering, has also amplified the peril of cybercrime and cyber-terrorism, posing significant threats to cyberspace. Consequently, cyberspace is increasingly being perceived as an inherently hazardous domain, necessitating heightened security measures and rigorous management. Despite the efforts of governments and international organizations in implementing various cybersecurity measures and regulations, there remains a pressing need for additional strategies. This paper endeavours to explore how we can foster collaboration between governments and citizens to safeguard and fortify our digital rights. Furthermore, it delves into recent national and international cybersecurity incidents on the Internet and examines external regulations aimed at countering cybersecurity threats.

Keywords: *cybersecurity, cyberspace, united nations, covid-19.*

INTRODUCTION

In the modern world, our daily activities, such as business transactions, banking, and shopping, heavily rely on cyberspace. The COVID-19 pandemic accelerated this dependence, as many

aspects of our lives shifted from physical to digital platforms. However, this increased reliance on the internet has also exposed us to cyber threats, raising significant security concerns for individuals and organizations. Cybersecurity has become a critical component of the information technology landscape, with the primary challenge being how to safeguard our information effectively in today's digital age. When we think about cybersecurity, the immediate concerns that come to mind are cybercrimes and cyber-terrorism. These digital crimes are on the rise, often making it difficult to identify the victims.

Governments and companies are taking various measures and implementing laws to counteract these cyber threats. Emerging technologies like online banking, e-commerce, mobile computing, and cloud services offer convenience but also store sensitive personal information. Consequently, there is a pressing need to bolster cybersecurity efforts to protect individual privacy. Furthermore, enhancing cybersecurity and safeguarding critical information is vital for national security and economic stability. To combat cybercrimes and ensure online security, governments must commit to comprehensive and proactive cybersecurity strategies. The fight against cybercrime necessitates a holistic and more robust security approach.

ANALYSIS

What exactly are Cyber-Security Threats?

Cyber-security threat means any threat that is related to a malicious attack on a computer unlawfully and seeks access to data illegally, disrupt digital operations or damage information. Cyber threats can originate from various actors and organised groups like corporates- group species, program hackers, organised terrorist groups, and criminal organisations.[1]

[1] 'Cybersecurity Threats and Attacks: All You Need to Know' (*Stealthlabs*, 04 December 2020) <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> accessed 02 September 2023

In pandemic times, we have seen many instances of high-profile cyber-security attacks on cyber-space,[2] for example: 'ISRAEL BASED PEGASUS SPYWARE' has recently hacked the mobile of famous journalists, actors and political parties. Cyber attackers can use Individual sensitive data to steal their information or gain to access financial account information.[3] Therefore with the increasing threats on the Internet, there is a need to make some advanced cyber security regulations and advanced security rules to protect personal information from criminals on cyber-space.

Some Cyber Security Threats are as follows:

Malware Attacks: It is malicious software for example ransomware and espionage attacks. This attack is activated when the victim/user clicks on the malicious app button or any malicious link which leads to install dangerous software on the user's PC program. This blocks the access network, installs harmful software and disrupts the individual's important files on their program.

EMOTET Malware:[4] It is a very advanced and prefabricated banking Trojan attack that functions as a downloader of other banking Trojans. It is very costly and dangerous malware software.

Denial of Service (DOS):[5] This attack is based upon shutting down the computer program or its network. Making it inaccessible to its intended users.

Man in the Middle: This attack place when the man is included in two-party transactions. The malicious cyber-attack interrupts the work through the internet, steals your data and can filter

[2] Dan Lohrmann, '2020: The Year the COVID-19 crisis brought a cyber- pandemic' (*Government Technology,* 11 December 2020) <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html> accessed 02 September 2023

[3] 'Pegasus Spyware used to hack phones of journalist, politicians in India' (*Times of India*, 18 July 2023) <https://timesofindia.indiatimes.com/india/pegasus-spyware-used-to-hack-phones-of-journalists-politicians-in-india-report/articleshow/84531126.cms> accessed 02 September 2023

[4] 'Let's talk about EMOTET malware?' (*Malwarebytes*) <https://www.malwarebytes.com/emotet> accessed 03 September 2023

[5] 'Understanding the Denial-of-service Attacks' (*Cybersecurity & Infrastructure Security Agency,* 01 February 2021) <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks> accessed 03 September 2023

the whole program from your phone or app. For example bank transactions, ATM payments, and network transactions.

Phishing: This attack includes fake communication such as email, message or other communication sources. The main aim of this attack is to trick the receiver into opening the mail and following the inside instructions after the whole process is done this attack withdraws the money from a bank or hacked personal information. Sometimes Phishing is converted into ransomware where money is demanded through crypto-currency. The main mission is to steal personal sensitive data like credit card information or install malware attacks on the victim program.[6] For instance, The JAMTARA is the new emerging case of Phishing.

Password Attacks: With the help of some trick or social engineering, the hackers attack on password of the victim and get some important and sensitive information from the computer program which can be sometimes very dangerous and harmful to the national integrity and security of India.

What is cyber-security?

Usually, Cyber security can be defined as the protection of systems networks and data in cyberspace. It refers to the preventive methods used to protect information from being stolen, compromised or attacked.[7] Any organisation before making any web or app should be protected from privacy and security of the data and this is always the top concern for any organisation.[8] The pandemic time plays a very important role in total dependency on the Internet and day by day this dependency on cyberspace has been extending due to this extension cybercrime has been taking new emerging threats called cybercrime and cyber terrorism. Therefore cyber security became the top issue to protect individual privacy or their property and threats related to nations. Social networking sites provide us with a space where users feel safe as they interact with friends and family. Day by day cyber-criminals are increasing and targeting emergency

[6] Sanjoy Dey, 'India's cyber-crime hub Jamtara scripting new story with public library mission' (*Hindustan Times*, 26 February 2021) <https://www.hindustantimes.com/india-news/indias-cyber-crime-hub-jamtara-scripting-new-story-with-public-library-mission-101614333756456.html> accessed 03 September 2023

[7] Mrs. Ashwini Sheth et al., 'Research Paper on Cyber Security' (2021) CONTEMPORARY RESEARCH IN INDIA

[8] INTERPOL, *Covid 19 Cybercrime Analysis Report August 2020* (2020)

national security like army telecommunication services. This is not only cyber networking but also during bank transactions a person must take all the required security measures.[9]

During the pandemic we have seen many cases related to cyber security where a hospital's patient data is leaked, a power system was hacked and comments a political leader posted on cyberspace which is also covered under personal identity theft so old law and measures are not sufficient to handle emerging cyber-crimes. Cyber security also includes government and businesses in particular trend to tend to frame cyber security.[10]

The IT Act 2000 characterises 'cyber security' as the insurance given to devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.[11]

LEGAL PROVISIONS FOR CYBER-SECURITY IN INDIA

India's legal framework for cyber security:

1. Indian Information Technology Act 2000:

- Section 65 (Tempering with Computer source)[12],
- Section 66 (Hacking and computer offences),[13]
- Section 43 (Tempering of electronic records).[14]

Indian Copyright Act: If there is any illegal activity done with the use of a Computer program with ill-will intention then that person would be punishable. Computer programs are protected by the copyright in computers but for patents, there is no such punishable mention in the Copyright Act.

---

[9] Ablgall K. Lelchman, 'Hospital Cyber-attack is the new pandemic; here's the cure' (*ISREAL21c*, 29 November 2021) <https://www.israel21c.org/hospital-cyberattack-is-the-new-pandemic-heres-the-cure/> accessed 03 September 2023

[10] Information Technology Act 2000, s 2(na)

[11] Information Technology Act 2000, s 2(nb)

[12] Information Technology Act 2000, s 65

[13] Information Technology Act 2000, s 66

[14] Information Technology Act 2000, s 43

2. Indian Penal Code 19860:

- Section 406 (Punishment for criminal breach of trust)[15],
- Section 420(cheating and dishonesty including delivery of property).[16]

Indian Government Initiatives:

National Cyber Security Policy 2013: The Indian government took the first steps related to cyber security in 2013. The main aim of this policy is to build a secure and resilient cyberspace for citizens, businesses and the government. The main purpose of this policy is to maintain the ecosystem in cyberspace, secure it from cyber threats as well and protect it from outside institutional threats. This policy is also focusing on national critical infrastructure from national critical infrastructure cyber threats.

Cyber 'Swachhata' Kendra 2017 (Botnet Cleaning and Malware Analysis Centre): To protect from cyber security violations and their increase, the government of India launched 'CYBER SWACHHTA KENDRA' in 2017, also known as Botnet Cleaning and Malware Analysis Centre. The main mission of this policy is to detect botnet infections in India and prevent further infections by notifying, enabling cleaning and securing systems of end-users.

USB Pratorodh:[17] The main purpose of this policy is to control the unauthorised usage of removable USB storage media devices like pen drives, external hard drives and USB-supported mass storage devices. This policy was launched by the government, Union IT and Electronics Minister Ravi Shankar Prasad.

SAMVID App: The app is a desktop-based application whitelisting solution for the Windows operating system. It allows only preapproved and executable files for execution and protects desktops from suspicious applications from running.

---

[15] Indian Penal Code, 1860, s 406
[16] Indian Penal Code, 1860, s 420
[17] 'USB Pratirodh is a free security tool to control usage of removable USB storage media' (*The Windows Club*) <https://www.thewindowsclub.com/usb-pratirodh-control-usb-usage> accessed 05 September 2023

WHY THE WORLD NEEDS A CYBER UNITED NATIONS-LIKE BODY CYBER-WHO TO COUNTER VIRUSES IN CYBERSPACE

'In the year of a pandemic, the global nations have helped developing countries from COVID-19, But the global nations need to work on less technologically advanced countries and need to protect against the risk of the plague of cyber-attacks from less technological countries.'[18]

For instance, Solar Wind Software hacked in the US: Recently there was news related to a cyber-attack on 'Solar Wind'. In this attack, the hacker accessed Solar Winds software in U S and this software was hacked by thousands of large organized hacked groups with the help of a backdoor to enter cyberspace networks at several US federal agencies and private companies including Microsoft. Here US agencies find that Russia was behind this mass hacking. The US is a developed and technological country but if this happened with other less advanced countries then what would happen? So as per the present scenario Cyber-attack has become a big issue, with this concern we need to regulate some strict laws and other countries should also tie their hand with each other.[19]

There are different reasons to join or not to join the United Nations body (CYBER-WHO) on cyber-security:

To identify the hackers in cyber-space: As we saw that the whole world is fighting against COVID-19, with the increasing risk of the pandemic we have to handle the risk of increasing attacks on cyberspace and have to find solutions to prevent it. The major risk these days in cyber-space is to identify the hackers so there is a need for advanced technological machines to defend from cyber-attacks.[20]

---

[18] Yaron Rosen, 'The World Needs a Cyber –WHO to counter viruses in cyberspace' (*Foreign Policy Magazine*, 24 January 2021) <https://foreignpolicy.com/2021/01/24/the-world-needs-a-cyber-who-to-counter-viruses-in-cyberspace/> accessed 05 September 2023

[19] Kevin Collier, 'Why the Russian hack is so significant, and why it's close to a worst-case scenario'(*NBC NEWS*, 23 December 2020) <https://www.nbcnews.com/tech/security/why-russian-hack-so-significant-why-it-s-close-worst-n1252131> accessed 06 September 2023

[20] Rosen (n 18)

COVID-19 health issue-related theft: In recent times we had many examples related to the identity of the patient which was hacked for malicious use. The reason behind identity theft is the lack of technological knowledge of victims because people use technological machines in emergencies so due to a lack of knowledge about advanced technology many people face and become the victim of cyber-attacks. So due to cyber-security concerns the less technological countries should take help from the World Health Organisation to identify such hackers.[21]

Dependency on Cyberspace: The internet has evolved into a complex digital landscape of websites, apps and other thousands of network providers and infrastructure nodes from satellites to WIFI routers. Due to total dependency on the Internet and virtual everything for example: cars to coffee makers. Therefore, the Internet world needs advanced technological machines and cyber-security.[22]

Ransomware attacks: With the advanced technological wave, physical ransomware has converted into Internet ransomware, we have seen many cases related to Ransomware where money is demanded by crypto-currency. U.S. states ransom-ware incidents in which the criminals restricted the health systems of victims and local government of US networks until they were paid.[23]

Personal information hacking: In India, the news appeared related to hacking the personal information of many famous people in 'Pegasus-Spyware' which is Israeli-based spyware, the main purpose of this spyware is to sell vetted government for national security purposes but what happened with this spyware, this spyware has used for personal purpose to hacked famous and political people for their own malicious purpose so there is a need to think about

[21] Lelchman (n 9)
[22] Rosen (n 18)
[23] *Ibid*

strict norms for cyber-security.[24] In another example, some sites, apps and personal information of U.S. people were hacked by North Korea via zero cyber-attack.[25]

There are some reasons why we need the cyber-WHO or reasons to deny the CyberWHO:[26]

- We need a cyber-WHO that is a global body that could develop norms about behaviour in cyberspace.
- To create incentives for nations to join, a cyber-WHO could provide the help of cyber safety rating and credit rating agencies and also help economies.
- If developing countries share information on health-related then there is a risk of disclosing personal information with developed countries. The countries like Iran and South Korea have refused to participate in such a body.
- The second risk to coordination with Cyber-WHO is Banks' personal information, if there is any threat related to banks in cyberspace then there is the chance to disclose all personal information of citizens and here security risks can take place instead of reducing cyber-threats.
- A cyber-WHO would ask participating nations and companies within them to share information on digital information on digital signatures and where possible attribution.
- It is fair to assume that the most advanced cyber countries would not share all the details of their technologies and methods with underdeveloped countries.

CASE STUDIES

State of Tamil Nadu v Suhas Katti (2004):[27] This was the first case that gave prime importance to section 65B[28] of the Indian Evidence Act and also this was the first case in India that was

[24] Bhanukiran Gurijala, 'what is Pegasus? A cyber-security expert explains how the spyware invades phones and what it does when it gets in' (*The Conversation*, 09 August 2021) <https://theconversation.com/what-is-pegasus-a-cybersecurity-expert-explains-how-the-spyware-invades-phones-and-what-it-does-when-it-gets-in-165382> accessed 05 September 2023

[25] Lucas Ropek, 'A Pisses-Off American Hacker Claims He Took Down North Korea's Internet All By Himself' (*Gizmodo,* 2 February 2022) <https://gizmodo.com/american-hacker-claims-he-took-down-north-koreas-intern-1848468102> accessed 05 September 2023

[26] Rosen (n 18)

[27] *Suhas Katti v State of Tamil Nadu* CC No 4680/2004

[28] Indian Evidence Act 1872, s 65B

related to obscene messages in cyberspace. This case was the benchmark in the cyber harassing issue in cyber-space. The question involved in this case was cyberstalking and harassing a woman in cyberspace using social media websites and fake mail. The woman filed the case based on obscene messages through mail by fabricated identity, the message was in very vulgar language and defamed of modesty of the victim. The judge passed the judgment in the favour of the victim on the basis of fact and circumstances and the accused was sentenced under sections 469[29], 509[30] and 67[31] marked that such crimes are very shameful and not only against the legality of the country but also against the modesty of the morality of the women.

NSP Bank Case:[32] This case was one of the leading cases which was related to Bank which was related to cyber phishing case. Here the couple exchanged many emails through the company's computer but sometimes Couples broke up and the accused (girl) created a fraudulent email ID such as Indian Bar Associations and through this fraud creation sent some emails to foreign clients. The accused used the bank computer to do this. Here the boy has lost many clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

Wannacry Ransomware (May 2016):[33] The year 2017 was the Ransomware attack on cyberspace. It was the first time the word 'ransomware' came into existence. On 12 May 2017, the updated version called 'WCRY OR WANNACRY' ransomware targeted the hospitals in the United Kingdom's National Health Service centre. The main purpose was of this attack to target the high profile around the world. Under this attack, the victim got the message through email or message where the message was like ransom-ware and this demand can be in Bit-coin mode. The criminal didn't give any guarantee to victims that their files would be decrypted after receiving the money.

[29] Indian Penal Code 1860, s 469
[30] Indian Penal Code 1860, s 509
[31] Indian Penal Code 1860, s 67
[32] *Syndicate Bank v NSP Associate India Pvt Ltd* IA 5624/2021
[33] David Bisson, '10 of the Most Significant Ransomware Attacks of 2017' (*TRIPWIRE*,10 December 2017) <https://www.tripwire.com/state-of-security/10-significant-ransomware-attacks-2017> accessed 07 September 2023

Jamatara' Karmatar and Harayana's Mewat Cybercrime Case:[34] We have read about a mass cybercrime hub in 'Jamtara' where bank fraud became the trend in the whole district as now the new location relating to cybercrime found in Haryana and Rajasthan where 70% of the recent cases set the alarm.

RECOMMENDATIONS TO SECURE DATA FROM CYBER THREATS

Strong Password Security: The easiest to secure your data from cyber-attacks is strong password security which should start from critical numbers and language so the hackers cannot break the code of your data.

Avoid unnecessarily spam messages and calls: The second technique avoid unnecessary messages on mail or message and any fake calls.

Anti-virus software: Installing anti-virus software from your PC software is the top solution to save your data for a long time. A good anti-virus software will provide daily base updates and be compatible with the system.

Firewalls: A software program or part of hardware that helps sort hackers, viruses and worms that attempt to reach your device over the web. Firewalls are also a good source to examine the waste messages incoming or leaving from our PC program. The main work of firewalls is to delete or reject the message which is unnecessary and can be hacked into your PC program.

Malware Scanners: Software that tests malicious code of harmful viruses in all files present in the device. Trojans, malware attacks, and espionage attacks are the major examples of cyber threats. So, our devices should be installed with original malware scanners to avoid such cyber threats in cyberspace.

Regular update and use with caution: Hackers can abuse your mail and web in many ways. So use your device with care and caution. Updating the system and periodic backup program is an

[34] Sharmita Kar, 'Is Mewat Turning Out to Be New Jamtara In Cyber Frauds?'*(INDIA.com*, 10 April 2021) <https://www.india.com/news/india/is-mewat-turning-out-to-be-new-jamtara-in-cyber-frauds-4574973/> accessed 07 September 2023

incredible process and guarantees that your information can be retrievable and protected from any bugs.

CONCLUSION

The study clearly that cyber security measures like using a firewall, strong passwords, installing original antivirus, not clicking unwanted mail and updating your device from time to time can give protection from cyber threats whereas, with the increasing use of technology on a mass level, the Indian government should amend some regulations and accept outside convention like 'Budapest Security Conventions'[35] and CYBER-WHO so that advance super power cyber country can help poor technological countries and can also help to secure their important data which is related to personal identity and national security of India. The idea of a 'Cyber WHO' (World Health Organization) has been proposed in response to the growing global challenges posed by cyber threats and cybersecurity issues. The concept has gained traction due to several compelling reasons.

In Conclusion, the world needs a 'Cyber WHO' for the following key reasons:

Global Interconnectedness: In today's interconnected world, cyber threats and vulnerabilities transcend borders. An international body like a Cyber WHO would facilitate collaboration among nations, fostering a collective approach to addressing cyber threats.

Emerging Threats: Cyberattacks are evolving rapidly in scale, complexity, and impact. A dedicated organization can pool resources, intelligence, and expertise to stay ahead of these threats and develop coordinated responses.

Protection of Critical Infrastructure: Many nations rely on interconnected critical infrastructure systems (e.g., energy, transportation, healthcare) that are vulnerable to cyberattacks. A Cyber WHO could help establish and enforce standards for securing these vital systems.

[35] Alexander Seger, 'India and the Budapest Convention: Why not?' (*Observer Research Foundation*) <https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/> accessed 07 September 2023

Capacity Building: Developing countries often lack the resources and expertise to effectively combat cyber threats. A global organization can provide support, knowledge sharing, and capacity-building programs to help these nations improve their cybersecurity posture.

Information Sharing: Cyberattacks often target multiple countries simultaneously. A Cyber WHO could serve as a clearinghouse for sharing threat intelligence, helping nations to better understand and mitigate threats in real time.

Norms and Regulations: A Cyber WHO could play a crucial role in establishing international norms and regulations governing cyberspace. This could help deter malicious actors and provide a legal framework for addressing cybercrimes.

Public Awareness: An international body focused on cybersecurity could raise awareness about cyber threats, promote responsible behavior online, and educate individuals and businesses on best practices for staying safe in the digital realm.

Crisis Response: In the event of a large-scale cyber incident with global implications, a Cyber WHO could coordinate a swift and effective international response, minimizing the damage and ensuring a coordinated effort to restore normalcy.

In light of these compelling reasons, the establishment of a 'Cyber WHO' or a similar international organization dedicated to cybersecurity and digital health is a logical step to address the growing challenges in our interconnected world. Such an entity would not only enhance global security but also contribute to the responsible and sustainable development of the digital age.