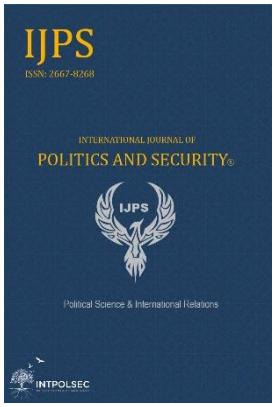
International Journal of Politics and Security (IJPS)

ISSN: 2667-8268

https://dergipark.org.tr/tr/pub/ijps



Emerging Cyber Security Threats: India's Concerns and Options

Author(s) / Yazar(lar) : Alik NAHA

Source / Kaynak: International Journal of Politics and Security (IJPS) / Vol. 4 / No. 1 / May 2022, pp. 170-200.

DOI: 10.53451/ijps.996755

Date of Arrival **:** 17.09.2021
Date of Acceptance **:** 30.03.2022

To cite this article:

Naha, Alik. "Emerging Cyber Security Threats: India's Concerns and Options". *International Journal of Politics and Security (IJPS)*, Vol. 4, No. 1, 2022, pp. 170-200, DOI: 10.53451/ijps.996755.

IJPS, 2022: 4(1):170-200
International Journal of Politics and Security, 2022: 4(1):170-200

Emerging Cyber Security Threats: India's Concerns and Options

Alik NAHA*

Abstract

It has been believed that cyber power, along with conventional aspects such as economic resources and political will, is becoming a key component of national power. According to this logic, the country that can best lead and control cyber power would be more powerful than others. Cyber terrorism has arisen as a new phenomenon in India and investigations about terror attacks revealed the cyber terrorism trials. Furthermore, the reliance of government organizations, businesses, economic operations, and military affairs on Information and Communication Technology (ICT) demands the inclusion of cyber technology in strategic calculations. So, this essay recons to building cyber power capacity may be used as a tool of Indian foreign policy, leveraging the experience and human resources in the area, as well as enhancing local and global cyber cooperation.

Keywords: *Cyber Warfare, Cyber Terrorism, India, National Security, Pakistan.*

Yeni Siber Güvenlik Tehditleri: Hindistan'ın Endişeleri ve Seçenekleri

Özet

Siber gücün, ekonomik kaynaklar ve siyasi irade gibi geleneksel yönlerle birlikte, ulusal gücün önemli bir bileşeni haline geldiğine inanılmaktadır. Bu yöndeki inanç özellikle son yıllardaki terör saldırılarının niteliğiyle oldukça pekişmiş ve siber güvenliğe verilen önem artmıştır. Bu mantığa göre siber gücü en iyi yönetebilecek ve kontrol edebilecek ülke diğerlerinden daha güçlü olacaktır. Bu kapsamda siber terörizm Hindistan'da yeni bir fenomen olarak ortaya çıkmış ve terör saldırılarına ilişkin soruşturmalar siber terörizmin izlerini ortaya çıkarmıştır. Ayrıca, devlet kurumlarının, işletmelerin, ekonomik operasyonların ve askeri işlerin Bilgi ve İletişim Teknolojisine (BİT) güvenmesi, siber teknolojinin stratejik hesaplamalara dahil edilmesini gerektirir. Bu nedenle, bu makale, siber güç kapasitesinin oluşturulmasını, bölgedeki deneyim ve insan kaynaklarından yararlanmanın yanı sıra yerel ve küresel siber işbirliğini güçlendirerek Hindistan dış politikasının bir aracı olarak kullanılabileceği üzerinde duruyor.

Anahtar Kelimeler: *Siber Savaş, Siber Terörizm, Hindistan, Ulusal Güvenlik, Pakistan.*

1. Introduction

Security is a key aspect in the study of IR. Until recently, security analysis was primarily concerned with state security, considering it as a consequence of the degree of dangers that states confront from other states, as well as the method and efficacy with which governments respond to such threats.[1] However, in the post-Cold War era, researchers changed their attention away from the state-centric definition of security, broadening the concept to encompass

* Faculty Member, Department of Political Science Vidyasagar College, Kolkata/India. aliknaha@gmail.com, ORCID: 0000-0002-2171-6900
Date of Arrival: 17.09.2021 – **Date of Acceptance:** 30.03.2022.
[1] Mohd Aarif Rather an Kishor Jose. "Human Security: Evolution and Conceptualization." *European Academic Research* 2, no.5 (2014): 6766–6797.

individual security.[2] National security, under this new view, began to include security issues moving beyond the conventional notion of territorial protection, such as poverty, industrial competitiveness, lack of basic education, environmental challenges, illegal drug & human trafficking, and resource scarcity. Furthermore, as a result of the technological revolution that began with the turn of the century, human lives have changed dramatically, as have the dangers to their lives and national security.

The next era's realpolitik is "*cyber-politik*".[3] Actors have evolved beyond the traditional notions of state and military power, and they are now challenged or forfeited by cyber power. The influence of Julian Paul Assange, editor in chief of Wikileaks, on political circles throughout the world is only one example of the wide range of players enabled by ICT. Multinational companies (MNCs) and certain non-governmental organizations (NGOs) are increasingly free to act worldwide with little regard for the needs of particular states. The international community also regards the use of nuclear weapons as having the devastating force of conventional weapons, making their deployment on a wide scale nearly unthinkable. In this information era, non-lethal weapons (NLW) in the form of cyber warfare are viewed as more benign yet effective instruments for wielding power.

Indeed, in this technocratic era, national security is confronted with hitherto unknown dangers aimed at destroying a state's infrastructure. It is a fact that technology, more so modernization is critical for economic and social growth in a globalized society, providing an advanced technology-based infrastructure is necessary for societies, businesses, and governments to fulfill their fundamental tasks. But the vast realm of the internet which is beyond surveillance makes it an unsafe environment on several levels.[4] Cyber threats are developing and multiplying at an alarming rate this decade. They are not just launched by dark web criminals, but also emerge from sources, such as enemy nations and political parties, and may be motivated by reasons other than profit. This latter category may encompass political hacktivism, political instability, cyberespionage, sabotage, and even military activities.[5]

[2] Barry Buzan. *People, States, and Fear: An Agenda for International Security Studies in the Post Cold War Era*. (London: Harvester Wheatsheaf, 1991).
[3] M.K. Sharma. "Cyber Warfare: Implications for India." *In India's National Security Annual review 2011,* ed. *Satish Kumar*, (Routledge: 2011).
[4] P. Pillai. 2012. "History of Internet Security."
[5] Sushma Devi Parmar. "Cybersecurity in India: An Evolving Concern for National Security." *The Journal of Intelligence and Cyber Security* 1, no.1 (2018).

Human beings are susceptible to difficulties ranging from life danger to troubles at a time when individual privacy is at an elevated risk of violation owing to trojans, viruses, malware, unethical hacking, data outrage, and so on. Confidential information from public and private enterprises, defense forces, security institutions, hospitals, and online or retail shops is exposed to cyber-attacks since it may be exploited for both financial and strategic advantage. As a result of the advancement and complexity of cyber-warfare technologies, there is a growing need to implement security measures to protect individual data and national security.

Thus, Cyber-security may be defined as "*the collection of tools, policies, guidelines, training, actions, security concepts and safeguards, risk management approaches, assurance, and technologies that can be used to secure and protect the cyber environment as well as the organization and user assets*.".[6] Its goal is to protect information technology, data, computer programs, and networks, as well as to limit unwanted access to information and prevent unintended alteration or destruction. Making the Internet as safe as feasible is increasingly important to government policy in a world where sophisticated communication and technical infrastructure are critical to security and economic progress.[7] On the other hand, Joseph Migga Kizza characterized cyber security as consisting of three elements: confidentiality, integrity, and availability. Traditional criminal behaviors like theft, fraud, forgery, defamation, and mischief, all of which are covered under the Indian Penal Code, might be included in cybercrime. The Information Technology Act of 2000 addresses a variety of new-age offenses that have arisen as a result of the misuse of digital technologies. The Information Technology Act, 2000 (also known as ITA-2000 or the IT Act) is an Indian Parliament Act (No 21 of 2000) that went into effect on October 17, 2000. It is India's fundamental law governing cybercrime and electronic commerce. In 2008, this act was significantly amended. It enacted Section 66A, which made it illegal to send offensive messages. It also included Section 69, which empowered authorities to intercept, monitor, or decode any information through any computer resource. It also imposed sanctions for child pornography, cyber terrorism, and voyeurism at the same time.

[6] *Ibid.*
[7] Marco Gercke. Understanding Cybercrime: A Guide for Developing Countries. (Geneva: ITU Publication, 2009)

Given this context, the paper has focused on four research questions:

a. How is India vulnerable to this emerging threat of cyber warfare and its concerns over cyber-terrorism?

b. How does the Sino-Pakistan cyber nexus pose an imminent challenge to Indian security?

c. Has India benefitted in cyberspace security through cooperation with the US and Russia?

d. How has the pandemic boosted cyber crimes against India?

1.1. Methodology

The current research was carried out using content analysis and observation techniques. Based on a review of secondary data sources such as books, book chapters, journals, papers, and other pertinent sources related to this research. The key arguments of the study were built using these sources of information.

1.2. Literature Review

Cyber security is a subset of IT security. Unauthorized access, attack, and destruction of digital data on your networks, computers, and devices are all protected by cyber security. Cyber security protects the digital data on your networks, computers, and devices from unauthorized access, attack, and destruction. While IT security protects both physical and digital data, cyber security protects the digital data on your networks, computers, and devices from unauthorized access, attack, and destruction. S W Brenner (2004)[8] in her article titled "*Cybercrime metrics: old wine, new bottles*", outlines the first strategy for identifying measures for assessing cybercrime. Despite the fact that defining measurements and scales for cybercrime is exceedingly challenging due to apprehension, scale, and evidence concerns, she proposes a simple taxonomy of harms consisting of three types: individual, systemic, and collective. Chertoff et al. (2015)[9] discuss the current condition of Internet jurisdiction law, as well as the difficulty of allocating legal authority to a specific forum when a lawsuit crosses many states. They give four different formulations for clearly and fairly establishing the dominant

[8] Susan W. Brenner. 2014. Cybercrime metrics: old wine, new bottles? Virginia Journal Oflaw & Technology 9, no.13 (2014): 1-52.
[9] Michael Chertoff and Paul Rosenzweig. "A Primer on Globally Harmonizing Internet Jurisdiction and Regulations." (2015).

jurisdiction in situations. The citizenship of the offending information, data, or system's subject, the location where the harm happened, the citizenship of the data producer, or the citizenship of the data holder or custodian are all factors under these regulations. By focusing on the victimization aspect of white-collar crimes, Van Slyke et al. (2016)[10] construct a taxonomy of harms for these crimes. According to Ghate and Agarwal (2017)[11], cyber security refers to the technology, methods, and practices used to safeguard computers, programs, networks, and data from being hacked, damaged, or accessed without authorization. In public debates, cyber security is sometimes confounded with other ideas such as privacy, information exchange, intelligence collecting, and surveillance. Through its Task Force Report on India's Cyber Security Challenge (2012)[12], the Manohar Parrikar Institute for Defense Studies and Analyses (MP-IDSA) presented a detailed review of India's position in the area of cyber security. In a highly scientific approach, this study has detailed the Indian cyber scenario, loopholes, and strategies required to tackle the Internet war (IW) and Cyber War (CW). It has also offered a possible office structure that may be necessary to play a vital role in the event of IW and CW.

2. Conceptualizing Cyber Terrorism

The concept of cyber-terrorism may be traced back to the early 1990s when a fast increase in Internet use and discussion over the developing "information society" prompted many studies on the possible hazards confronting the increasingly networked, high-tech-dependent United States. Psychological, political, and economic pressures have all worked together to instill fear of cyber-terrorism.[13] Dread of random, violent victimization combines well with skepticism and open fear of computer technology. An unknown threat is believed to be more dangerous than a recognized threat. Although cyber-terrorism may not pose a direct danger of violence, its psychological impact on nervous communities can be just as potent as terrorist explosives. According to former US President Barack Obama, cyber threat is one of the most significant economic and national security threats that a country faces in modern times.

[10]Shanna Van Slyke, Michael L. Benson, The Oxford Handbook of White Collar Crime. (Oxford University Press, 2016).
[11] S. Shweta Ghate And Pragyesh Kumar Agrawal. "A Literature Review on Cyber Security in Indian Context", *Journal of Computer & Information Technology* 8, no.5 (2017): 30-36.
[12] MP-IDSA. (2012). India's Cyber Security Challenges. New Delhi. Accessed September 1, 2021.https://idsa.in/system/files/book/book_indiacybersecurity.pdf
[13] Gabriel Weimann. Cyberterrorism: How Real Is the Threat? (Washington D.C.: United States Institute Of Peace, 2004). Accessed September 1, 2021. www.usip.org.

The phrase "cyber-terrorism" was coined in the late 1980s by Barry C. Collin. It is a broad word. There have been several roadblocks in developing a clear and uniform definition of the word "cyberterrorism". First, most of the debate about cyberterrorism has taken place in the popular media, where journalists are more concerned with drama and sensation than with clear operational definitions of new words. Second, while working with computers, it has been very popular to coin new terms simply by adding the words "cyber", "computer", or "information" before another word. Thus, a slew of terms—cybercrime, info-war, netwar, cyberterrorism, cyber harassment, virtual warfare, digital terrorism, cyber-tactics, computer warfare, cyberattack, and cyber-break-ins—are employed to describe what some military and political strategists refer to as the "new terrorism" of our times.

Dorothy Denning characterized cyber-terrorism as the fusion of cyberspace and terrorism. It refers to unlawful assaults and threats of attacks on computers, networks, and the information stored on them that are carried out to intimidate or compel a government or its people in the pursuit of political or social objectives. Furthermore, to qualify as cyberterrorism, an attack must result in violence against people or property, or at the very least do enough harm to induce fear. Attacks resulting in death or bodily harm, explosions, or significant economic damage are instances. Depending on the severity of the assault, serious cyberattacks against vital facilities might be considered acts of cyber-terrorism. dreadful attacks.[14] According to the United States Federal Bureau of Investigation, cyber terrorism is any premeditated, politically motivated attack on information, computer systems, computer programs, and data that results in violence against non-combatant targets by subnational organizations or clandestine operatives.[15] The North Atlantic Treaty Organization (NATO) has defined cyber-terrorism as "*A cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal*."[16]

Multiple web-based techniques and methods are employed to carry out cyber-terrorism. This may include:

[14] Ibid.
[15] Amaresh Pujari. Cyber Terrorism: World Wide Weaponisation! Tamil Nadu Police Sesquicentennial Anniversary Souvenir, (2017).
[16] Centre of Excellence Defence Against Terror, NATO Science for Peace and Security, (IOS Press; 1st ed., 2008)

a. *Hacking* - Hacking is the term used to describe operations that attempt to infiltrate digital devices such as computers, cellphones, tablets, and even whole networks. These are illegal actions carried out by cybercriminals for financial gain, protest, or information collection (spying). Hacking is encouraged by certain component automation such as packet inhaling storm assault, password crash, and bulwark depletion.[17]

b. Trojans- A Trojan horse, often known as a Trojan, is a kind of malware that is frequently disguised as genuine software. Cyber-criminals and hackers may use Trojans to obtain access to users' computers. Trojan viruses are classified into several kinds, including Cryxos Trojan, Banker Trojan, Clampi Trojan, DDoS Trojan, FakeAV Trojan, and others.

c. Computer Worms - A computer worm is a form of malware that replicates itself and distributes it from computer to computer. A worm can replicate itself without the need for human intervention, and it does not need to be attached to a software application to inflict harm.

d. E-Mail Spams - A spam email is an unsolicited and undesired junk email that is sent in mass to a random recipient list. Spam email may be harmful. It may include dangerous URLs capable of infecting your machine with malware. They are the most effective spreaders of web-based viruses and worms. They are also used to disperse distortion, terrors, and insulting content.[18]

e. *Denial of Service* - A Denial-of-Service (DoS) attack aims to put a system or network to a stop, leaving it inaccessible to its intended users. DoS attacks do this by bombarding the target with traffic or delivering information that causes it to crash. A denial of service, for example, is common in any online-based sales when thousands of individuals are screaming for a discount. They can, however, be malevolent. In this case, an attacker tries to deliberately exhaust the site's resources, preventing legitimate users from accessing it.

3. Vulnerability to Cyber Warfare

Indian policymakers have mostly ignored the problem of cyber-security. India lacks the strong cyber-security mechanisms needed to combat the rising threat of cyber-terrorism, of which India is a major victim. According to Kaushik (2014), India's capacity to combat complex

[17] Saheli Naik. "A Biggest Threat to India – Cyber Terrorism and Crime." *Journal of Research in Humanities and Social Science* 27, (2017): 27-30.
[18] Ibid.

malware such as Stuxnet, Flame, and Black Shades is hampered by a lack of comprehensive offensive and defensive cyber-security measures.[19] Furthermore, as compared to other advanced countries, India has much fewer cybersecurity programs and efforts. Many of the important projects planned by the Indian government is far from being actualized. Furthermore, important initiatives such as India's National Critical Information Infrastructure Protection Centre (NCIPC) and National Cyber Coordination Centre (NCCC) are yet to be operationalized.[20] Furthermore, much to the dismay of many, the National Cyber Security Policy (2013) has failed to yield productive results, as its execution appears to be lacking in a variety of areas, including violation of privacy and individual rights.

Indeed, the Indian government has acknowledged a significant increase in cyberattacks on businesses such as the banking and financial services sectors. For example, while the country ranks 85th in the world in terms of internet access, it ranks 9th in terms of cyberattacks. Surprisingly, almost 1.16 million cyberattacks were recorded in 2020, nearly three times the number reported in 2019 and more than 20 times the number reported in 2016.[21] An average of 3,137 cyber-security issues were reported every day of the year. According to official data, between September and December, roughly 115,000 cyber-attacks were registered per month. Between January and August of last year, 696,938 cyberattacks were reported, according to police. The Indian Computer Emergency Response Team (CERT-In) has experienced significant growth in cyber security threats in recent years. According to research firms and experts, such assaults are expected to increase in 2021, and they may occur in any industry, including manufacturing, services, education, and healthcare. As a result, to address these critical security challenges, India must develop an efficient cyber-security management plan.

The information technology sector is a key contributor to India's economic growth. TCS, Infosys, WIPRO, and other IT behemoths play critical roles in expanding India’s prominence as a major global software developing nation as well as in delivering commercial solutions. This expansion is accompanied by the requirement to create a safer virtual environment by

[19] R.K. Kaushik. "Cyber Security Needs Urgent Attention of Indian Government.", 2014. Accessed September 2, 2021. http://cybersecurityforindia.blogspot.in/2014/09/cyber-security-needs-urgent-attention.html.
[20] Sushma Devi Parmar. "Cybersecurity in India: An Evolving Concern for National Security." *The Journal of Intelligence and Cyber Security* 1, no.1 (2018).
[21] Prashant K. Nanda. "Cyberattacks surged 3-fold to 1.16 mn last year in India." (2021). Mint, March 23. Accessed September 2, 2021. https://www.livemint.com/news/india/as-tech-adoption-grew-india-faced-11-58-lakh-cyberattacks-in-2020-11616492755651.html.

instilling trust and prioritizing the security of this sector. For example, today's banking and business sectors are embracing more and more technologies to provide robust and simple customer service, therefore encouraging prospects for development, but they are also becoming increasingly exposed to cyber-attacks, the mitigation of which remains a concern.[22]

Critical sectors such as military, banking, energy, telecommunications, transportation, and other public agencies rely significantly on computer networks to transmit data for transactions as well as a source of information and communication.[23] To date, the government has ambitious ambitions to expand e-commerce services, cyber connections, and overall IT use in communications. In this respect Prime Minister Modi's greater emphasis on digitalization and promotion of e-governance is crucial. He observed, "*Digital India… aims to connect all gram panchayats by broadband internet, promote e-governance and transform India into a connected knowledge economy*."[24] One of the major objectives of the program undertaken in 2014 was to bring the 30,000-crore telecom endeavor for offering community wi-fi services through the forthcoming National Optic Fiber Network (NOFN) initiative to fruition. Such initiatives and efforts required strong cyber-security policies to mitigate future threats.

To address the issue of confidential data theft critical to national and strategic security perpetrated by hackers and other nations, various organizations within the purview of the Ministry of Defence have taken on the task of dealing with cybersecurity. For example, the Indian Army established the Cyber Security Establishment (2005) to secure the army's networks at the divisional level and to perform safe cyber-security assessments. According to India's Army officials, Guarding the air, land, and sea is no longer deemed enough because national borders are irrelevant in cyberspace.[25] In addition to military assets, well-executed cyber-attacks may cripple a country's power grids, banking, communication, and other networks. Given the importance of cyber-security, the Signals Corps has created a "*center for excellence*" in this field at its training facility, the Military College of Telecommunication Engineering at

[22] S. Jain. "Cyber Security: A Sine Qua Non.", (2014), Accessed September 2, 2021. http://www.indiandefencereview.com/news/cyber-security-a-sine-qua-non/.
[23] Sushma Devi Parmar. Cybersecurity in India: An Evolving Concern for National Security.
[24] ET Bureau. "Government Mulls Digital India Programme to Connect All Villages." *The Economic Times*, 21 August 2014, https://economictimes.indiatimes.com/news/economy/policy/government-mulls-digital-india-programme-to-connect-all-villages/articleshow/40524106.cms. Accessed 02 September 2021.
[25] Rajat Pandit. "Army gearing up for cyber warfare." The Times of India, 7 July 2005, https://timesofindia.indiatimes.com/india/army-gearing-up-for-cyber-warfare/articleshow/1163080.cms., Accessed 02 September 2021.

Mhow.[26] The Ministry of Information and Communication released a draft of the National Cyber-security Policy in 2011, emphasizing critical infrastructure security and protection, development initiatives, and public-private partnerships.[27] Under the draft strategy, a proposal to construct the National Critical Information Infrastructure Protection Centre was developed the next year under the auspices of the National Security Council.[28] Also in May 2012, India's DRDO created an indigenous cyber defense system to protect the safety and security of network sectors.[29] Simultaneously, the Technical Intelligence Communication Centre and the National Defence Intelligence Agency formed a collaborative team to enhance government awareness of possible cyber risks.[30]

India's energy installments have been vulnerable to many cyber-attacks throughout the years. As a result, a major non-conventional threat to India's domestic security has developed. Information about cyberattacks and equipment vulnerabilities in the Indian energy sector is practically non-existent due to poor regulation of information sharing and insufficient organizational capacity to support it. However, based on global cybersecurity patterns, we may assume that the industry is increasingly being targeted by sophisticated assaults, particularly since India has begun to integrate it with modern technology to satisfy expanding energy requirements.[31] Indeed, with the gradual modernization of India’s energy program, the sector has become increasingly vulnerable to cyber-attacks. The essential infrastructure that underpins all economic activity in India is entirely dependent on the electricity industry; this sector's reliance on ICT has highlighted several cybersecurity issues. It is believed that 60 percent of all cyberattacks on India's automated power networks occurred between 1994 and 2004.[32] Northern India experienced a major blackout on July 30 and 31, 2012, disrupting over 670 million people's regular life and work and causing damage to all services in the region, including

[26] Ibid.
[27] DIETY. 2011. Discussion Draft on National Cyber Security Policy. New Delhi: Government of India.
[28] Josy Joseph. "India to Add Muscle to Its Cyber Arsenal." *The Times of India*, 11 June 2012.
[29] UNIDIR. The Cyber Index: International Security Trends and Realities. New York and Geneva: United Nations Institute for Disarmament Research, (2013).
[30] Harsimran Singh and Joji Thomas Philip. "Spy Game: India Readies Cyber Army to Hack into Hostile Nations Computer Systems." The Economic Times, 06 August 2010, https://economictimes.indiatimes.com/spy-game-india-readies-cyber-army-to-hack-into-hostile-nations-computer-systems/articleshow/6258977.cms?from=mdr., Accessed 02 September 2021.
[31] Michael Walstrom. India’s Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges. (Seattle: Henry M. Jackson School of International Studies, 2016).
[32] V. Ananda Kumar, Krishan K. Pandey and Devendra Kumar Punia. *Facing the Reality of Cyber-Threats in the Power Sector*. (Bangalore: Wipro Technologies, 2013).

road traffic and railroads.[33] The Times of India reported that in March 2021, *ten* Indian power assets and two Indian ports came under attack from China-linked cyber-hackers Red Echo. The power assets included

> "*Delhi State Load Dispatch Centre, DTL Tikri Kalan substation in Delhi, Mumbai Port Trust, Western Regional Load Dispatch Centre (WRLDC) in Maharashtra, NTPC's Kudgi power plant and Southern Regional Load Dispatch Centre (SRLDC) in Karnataka, VO Chidambarnar port in Tamil Nadu, Telangana Load Dispatch Centre, Eastern Regional Load Dispatch Centre in West Bengal and North Eastern Regional Load Dispatch Centre (NERLDC)in Assam*."[34] India's Energy Minister R.K. Singh informed Rajya Sabha, "*Some unsuccessful cyber attempts were reported from various agencies in the recent past. On receipt of such information, immediate measures are taken for isolation and other compliance measures by the respective organization*."[35]

The New York Times connected last year's grid collapse in Mumbai to Chinese hacking in a story published earlier this year. On February 12, this year, the National Key Information Infrastructure Protection Centre (NCIIPC), which handles India's cybersecurity activities in critical sectors, issued a warning regarding Red Echo attacking RLDCs and SLDCs.

4. The Threat of Cyber-Terrorism

Cyber terrorism is a subset of traditional terrorism in which the weapons are computer gadgets rather than firearms and ammunition. Both have the same goal in mind - to instill fear. Terrorism's primary goal is to create a ruckus by committing or inciting acts of violence throughout the world. In 1990, the National Security Council predicted that

> "*computers might be employed in the future not just to aid crime, but also as the principal tool for a criminal act. A computer is more powerful than a pistol in the hands of a robber. Terrorists may be able to cause more harm with a keyboard than a bomb in the future*."[36]

The internet provides terrorists with the following benefits: *first*, simple mapping of the place of the attack; *second*, a larger audience reach; *third*, Anonymity, in other words,

[33] Shuran Liu, Su Guo and Hui Deng. "Analyses and Discussions of the Blackout in Indian Power Grid." *Energy Science and Technology* 6, no.1 (2013): 61-66.
[34] Sanjay Dutta. "10 power assets, Mumbai, Tamil Nadu ports came under RedEcho cyberattack." The Times of India, March 2021. https://timesofindia.indiatimes.com/business/india-business/10-power-assets-mumbai-tamil-nadu-ports-came-under-redecho-cyberattack/articleshow/81337328.cms., Accessed September 6, 2021.
[35] Mint. 2021. "Centre says four load despatch units came under cyberattack." July 22. https://www.livemint.com/news/india/indias-four-regional-load-despatch-centres-faced-cyberattacks-govt-11626856955565.html., Accessed September 5, 2021.
[36] Shiv Raman and Nidhi Sharma. "Cyber Terrorism in India: A Physical Reality or Virtual Myth." *Indian Journal of Law and Human Behavior* 5, no.2 (2019): 133-140. Doi: http://dx.doi.org/10.21088/ijlhb.2454.7107.5219.5.

cyberterrorism is more anonymous than traditional terrorist techniques; *fourth*, easy dissemination of propaganda; and *last*, the quantity and variety of targets are tremendous. Cyber-terrorists may attack the computers and computer networks of governments, people, public utilities, private aircraft, and other entities.

Denning defines information warfare as activities aimed at protecting, exploiting, corrupting, denying, or destroying information or information resources to gain a major advantage, objective, or triumph over an enemy. As a result, it could be argued that cyberterrorism is an act of hacking, blocking, and/or computer contamination to restrict legally authorized persons from accessing computer resources in general, and/or to gain or obtain unauthorized access to any information that is 'restricted information' for state security, foreign relations, etc.[37] These are heinous crimes committed with the purpose of endangering India's security, sovereignty, and integrity or instilling fear in the hearts of the people.

Web-based apps are increasingly being used to initiate cyber assaults. Hackers from China, North Korea, and Pakistan and terror outfits target Indian government and commercial sector websites regularly. This tendency is progressively gaining traction as societies become more and more technocratic. In such a case, cyber security rules must be implemented to address these new types of problems. Unfortunately, companies, government and private infrastructure, and institutions in India pay little attention to these problems.

India's Indira Gandhi International Airport (IGI) was subjected to a cyber assault in August 2013. A malware known as 'technical snag' disrupted the functioning of terminal number three. This malicious malware was distributed remotely to breach the airport's security system. The cyber attackers attempted to exploit the security system's flaws. Their strategy was to spread the virus program through boarding gate check-in centers and finally to the operation of CUPPS (Common Use Passengers Processing System), which has a significant impact on "*online reservation systems, expected time of departure, and capacity of waiting for the lounge*."[38] VOIP or Voice Over Internet Protocol has become a new tool for cyber-attacks used by hackers. Coded SMS, fraudulent emails with spam links, fake apps, international untraceable numbers, and gaining access to victims' mobile or other electronic devices through remote

[37] Halder Debarati, Information Technology Act and Cyber Terrorism: A Critical Review (August 1, 2011). Available at SSRN: https://ssrn.com/abstract=1964261 or http://dx.doi.org/10.2139/ssrn.1964261
[38] Ibid. (same as 31)

access applications (like Any Desk & Team Viewer) are techniques used by these hackers to meet their ends. Cyber terrorists are increasingly employing methods such as DDOS (Distributed Denial of Service), Phishing, Vishing (VOIP Phishing), Buffer Overflow, IP Spoofing, and so on. DDOS is growing as a preferred weapon of offenders among these technologies. Cyber-attacks have expanded in complexity and geographical reach in recent years.[39] There has also been a significant increase in the number of attacks. Other factors contributing to the massive increase in cyber-attacks in recent years include the ease with which malicious software is available, terrorist groups' increasing technological skills, and the ever-increasing networking of critical infrastructure in developed and developing countries. Terrorists have the same level of internet competence as US government organizations, according to a report provided to the US Congress by CRS (Congress Research Service). According to the same source, Al-Qaeda has set up web forums for its followers to discuss their computer hacking abilities.

Terrorist organizations employ "*E-Jihad*" to transition from traditional terror methods to technology-based terror techniques. Similarly, the worldwide terrorist group Al-Qaeda used the internet to spread its wicked wings. Similarly, ISIS has altered the "terrorist world" by utilizing "social media". Terrorists disseminate their propaganda using a variety of channels, including the internet and social media platforms such as Facebook, Twitter, and WhatsApp. These social media channels make it simple for terrorist propaganda to propagate. Twitter banned over one lakh accounts associated with ISIS in 2016. IS defectors Abu Hajer al-Maghribi and Abu Abdullah al-Maghribi told the reporters of The Washington Post that ISIS has established its media network as the most powerful propaganda engine. Senior media personnel is considered "*emirs*" with the same rank as their military colleagues. They have a direct say in strategy and territorial choices. According to Abu Abdullah al-Maghribi, "*The media people…have the power to encourage those inside to fight and the power to bring more recruits to the Islamic State*."[40] Furthermore, following the Paris attacks, it was proven how

[39] Amaresh Pujari. Cyber Terrorism: World Wide Weaponisation! Tamil Nadu Police Sesquicentennial Anniversary Souvenir. (2017).
[40] Greg Miller and Souad Mekhennet. "Inside the surreal world of the Islamic State's propaganda machine." The Washington Post, 20 November 2015. https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92ddd2b_story.html., Accessed August 30, 2021.

ISIS commanders utilized videos and messages posted on the internet as propaganda materials not only to terrorize an enemy but also to command a worldwide audience.

Since early 2020, web-based propaganda content targeting Indian interests has been appearing more aggressively. Technical developments have resulted in militant and terror organizations gaining technological literacy. Kashmir, for example, provides an intriguing study of the movements of online and offline terror propaganda. In Kashmir, Internet blockades and 'downgrades' from 4G to 2G following the central government's abrogation of the state in August 2019 have prompted an intriguing question: is slower Internet access across the state a gauge for online propaganda to slow down?[41] According to Kaul and Shah, restricting internet access and slowing surfing speed has neither prevented nor reduced the pace of online propaganda. They argue,

> "*Extremist propaganda posted by militant groups on Telegram, Twitter, Facebook, WhatsApp, and other social media sites continues unabated, as malicious actors seek to take advantage of the paucity of credible sources reporting on the ground to spread disinformation and rumors*."[42]

Voice of Hind, an anti-Islamic State (IS) journal published in India, was followed by editions in Hindi, Bengali, and Urdu. The Hindi output provides an intriguing insight. To begin with, it is not aimed at Kashmir or the typical pro-IS sympathizer instances in India, which have primarily come from middle-class areas where English is widely read and written. The Hindi output is titled "गजवाये हिन्द की तैयारी" or "*Preparing for Wilayat Hind*".[43] It was written in a very basic version of Hindi to appeal to a Muslim readership in India's hinterlands. This may also be viewed as a mirror to Al Qaeda in the Indian Subcontinent (AQIS) outreach in the region, as AQIS propaganda channels were recently combined with Al Qaeda central's authority. For India, AQIS has a separate "hinterland" wing.

The internet arena for terrorist propaganda is now open in India, with few resources explicitly dedicated to research and public policy to address the gaps in these fast-evolving national security problems. Furthermore, a more active push is needed now to bring these

[41] Kabir Taneja. *From 4G to Languages: The Developing Online Jihadist Propaganda Network in India.* (New Delhi: Observer Research Foundation, 2020).
[42] Ayushman Kaul and Khalid Shah. "Indian government's 2G restrictions in Kashmir fail to curb online extremism." DFR Lab. 25 May 2020. https://medium.com/dfrlab/indian-governments-2g-restrictions-in-kashmir-fail-to-curb-online-extremism-ea7a461f71cd., Accessed September 11, 2021.
[43] Ibid. (same as 36)

problems to the forefront of security debates, particularly in India, which has a considerably busy and chaotic national security environment as well as major capacity constraints.

Mr. Srijit Banerjee, Cyber Expert and Director of Sharktel Infocom Pvt. Ltd mentions that user data from compromised websites are accessible for sale on the 'Dark web' or 'Tor web'[44]. He mentions that Big Basket's (an online supermarket) client information, including bank account information, was recently stolen and made public on the Dark web. He further claimed that hackers are becoming more cautious about their operations and are targeting areas where individuals are readily persuaded. He uses the examples of Facebook Marketplace and Instagram Ad segments to demonstrate how people may be readily enticed by low-cost high-end items. Users are given the cash-on-delivery option or other similar ways to generate confidence, but when a user clicks the link for purchasing such items, certain malware may be placed in the user's device that can clone the device as a whole and allow the hacker total access to the device. Mr. Banerjee emphasizes that this is becoming a serious risk for consumers since cloned gadgets can be utilized for anti-national actions while the victim is ignorant. He stated that consumers should exercise caution while using mobile or web-based applications. The ISPs are taking the appropriate precautions to prevent such subtleties, but the user has the most responsibility.

In addition, the investigation into the 2008 Mumbai terror attacks revealed the use of satellite phones to carry out cross-border terrorist activities. Terrorists used the "Google Earth" program to track the movements of security agents and social media to locate their targets. Furthermore, they use technology to "*convert aural impulses into data*," making it difficult for "*Indian defense personnel*" to pinpoint the source of information.[45] In this scenario, the terrorists employed communication services to help them in carrying out the slaughter rather than to hack or block the protected information. Intercepted texts obtained during the prosecution of the Mumbai attack case would prove that the radicals were communicating only to exercise their freedom of expression. However, when the communication is viewed as a whole, it can be shown that this speech was carried out to undermine India's peace, security, and sovereignty, and so loses its nature as a protected speech under Art 19A of the Constitution.

[44] Mr. Srijit Banerjee was interviewed by the author on 26th August 2021.
[45] Shiv Raman and Nidhi Sharma. "Cyber Terrorism in India: A Physical Reality or Virtual Myth." *Indian Journal of Law and Human Behavior* 5, no.2 (2019.): 133-140. Doi: http://dx.doi.org/10.21088/ijlhb.2454.7107.5219.5.

Oh, et al. (2010) demonstrated that, in addition to general websites providing information on Mumbai target areas, terrorists had extensively exploited tweets made by ordinary individuals to acquire knowledge about the present state of affairs. The majority of these posts were written in response to individuals being warned about sensitive locations.[46] From these considerations, it is clear that the current legislation fails to recognize the extent of terrorists' physical communication in cyberspace. This failure has encouraged even more terrorists to use the internet for their goals. Another prominent example is the 2011 Javeri Bazaar bombing in Mumbai.[47]

Criminals now have more options because of technological advancements. Cyberwarfare entails the attack and defense of information and information systems both during armed conflict and in a non-conflict situation. Information technology has risen to prominence as a new class of less-lethal military weapons. These flaws, when exploited by individuals, would target people to instill widespread terror in the hopes of achieving a political goal. In the words of former National Security Advisor M.K. Narayanan, India is on the cusp of a digital age and the widespread use of IT technology. The concern is that not only is it getting simpler to conceal one's identity online, but once virus programs are available on the open market, they may be purchased and reused by hackers anywhere around the globe.

To combat the threat of cyber-terrorism, the Government of India amended the IT Act of 2000 in 2008. Section 66F, which defines and characterizes cyber terrorism, was explicitly added to this law for this reason. In addition, sections 69, 69A, and 69B were adopted. Section 69 discusses the authority to issue directives for the interception, monitoring, or decryption of any information obtained through any computer resource; Section 69A discusses the authority to issue directives for the blocking of public access to any information obtained through any computer resource, and Section 69B discusses the authority to monitor and collect traffic data or information obtained through any computer resource. All of these parts might represent the communicational element of cyber terrorism, which is absent from the definition of cyber terrorism in section 66F. Even though the revised Act in 2008 includes measures to protect

[46] Onook Oh & Manish Agrawal and H. Raghav Rao. "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter." *Information Systems Frontiers* 13, no.1 (2011): 33-43.
[47] Debarati Halder. "Information Technology Act and Cyber Terrorism: A Critical Review".

personal data, prevent financial fraud, and limit offensive speech, the goal of limiting extremist use of cyber communications was not adequately met.

5. India-Pakistan Cyber Warfare

Pakistani nationalistic programmers and hackers appear to be using the internet to target adversaries, particularly India. Pakistani hackers, like Indian hacktivists, mostly targeted Indian government websites using mutilation techniques. Pakistani hackers, in particular, were eager to counter Indian hacking in the aftermath of events or explicit physical acts in the Indian state of Jammu and Kashmir. In November 2008, the Pakistan Cyber Army (PCA) took part for the first time in the mutilation of the Indian Oil and Natural Gas Company. The PCA utilized straightforward methods to deface India's websites. In February 2016, Pakistani Advanced Persistent Threats (APTs) started a phishing campaign targeting Indian embassies in Kazakhstan and Saudi Arabia, dubbed ‘Operation Transparent Tribe’. Trend Micro discovered in March 2016 that a similar hacker gang from Pakistan was behind ‘Operation C-Major’. On the other side, Indian hackers and ethical programmers are widely known in cyberspace for their activities in support of Indian national interests. Indian hacktivists and active programmers primarily destroyed Pakistani official websites. These programmers also announced covert attacks on Pakistani government websites and airports. These acts have generally been taken in retaliation for the annoyance caused by the Pakistani perpetrators.

According to M. Dunn, the process of securitization has unavoidably resulted in a shift towards the more end of the cyber-threat spectrum and increased discussion of cyber-warfare as the most essential component of cyber-threat. Cyber attackers from India and Pakistan targeted broadly similar items and targets. However, Indian and Pakistani hackers have a proclivity to attack each other’s governmental and media websites. When hackers targeted government websites, it reflected that they were doing it for political reasons, indicating that they wanted their actions to be noticed. Pakistani APT targeted primarily Indian military and strategic personnel for the sake of national security covert activities, but they also targeted other political and military substances in South Asia. While India’s APT mostly targeted Pakistani business enterprises and government institutions for cyber espionage.

According to a British news agency, in 2014, Pakistani hackers known as Team Madleets attacked 2118 Indian websites, including the Central Bank of India and the website

of Indian actress Poonam Pandey. The team Madleets wrote Pakistan Zindabad on its main page and set the National Anthem as background music. According to a British news agency, an Indian cyber security official claimed that in retaliation, Indian hackers attacked nearly 100 Pakistani websites.[48] Pakistani hackers conducted a massive cyber-attack on Indian websites in 2018. Border disputes between Pakistan and India have a significant impact on the cyber world. Pakistani hackers and programmers hacked and defaced a significant number of Indian websites, including prominent hosting providers, the Government of Gujarat website, and the official website of the Kerala Government. Pakistani hackers put a message on their home page stating that "*security is an illusion and that Pakistan Zindabad*".[49] Among the Indian security establishments, there is a growing suspicion of a Sino-Pak cyber alliance against India.

6. Chinese Cyber Warfare Capabilities & Indian Concerns

China is one of the major Asian countries that employ cyber warfare tactics extensively. China initiated a cyber-warfare program in 1995, and by 1997, they were working on computer viruses to execute tactical operations such as interrupting "*military communications and public broadcasting networks*."[50] With the dawn of the new century, Beijing formed a special tactical strategic unit vested with the task to "*wage combat through computer networks to manipulate enemy information systems spanning spare parts deliveries to fire control and guidance systems.*"[51] In 2010, the Chinese People's Liberation Army, or PLA, announced the establishment of a specialized "Information Protection Base" in charge of information network security.[52] Beijing's cyber-warfare units have been extremely active; however, it is sometimes difficult to link operations originating in China to any government agency or individual Netizens. Starting from the late 20th century, there have been reports of cyber-attacks against government websites in Taiwan, the US, and Japan. These assaults have mostly consisted of simple website disruptions and/or server crashes caused by Denial-of-Service (DOS) applications. By 2002, these assaults had evolved into more sophisticated methods of stealing

[48] News Desk. "Pakistani hackers attacked 2,118 Indian websites." 2014. Pakistan Todays.
[49] Ghulam Mustafa, Zainab Murtaza and Khadija Murtaza. "Cyber Warfare between Pakistan and India: Implications for the Region." *Pakistan Languages and Humanities Review* 4, no.1(2020): 59-71. DOI:10.47205/plhr.2020(4-I)2.5.
[50] Desmond Ball. "China's Cyber Warfare Capabilities." *Security Challenges* 7, no.2 (2011): 81-103.
[51] Jason Sherman. "Report: China Developing Force to Tackle Information Warfare." Defense News, 27 November 2000.
[52] China Review News.. "The People's Liberation Army's First Force on Strategic Information Support and Protection is Established." 20 July 2010.

sensitive and unclassified information by infecting computer systems with trojan horse viruses disguised as Microsoft Word and PowerPoint presentations.[53] From the late 1990s to 2005, the PLA conducted more than 100 military exercises, and a comparable number is likely to have been performed from 2005 to 2010.[54] Admiral Willard, the former Chief of US Pacific Command, highlighted it in his 2010 report to the US Congress,

> "*U.S. military and government networks and computer systems continue to be the target of intrusions that appear to have originated from within [the People's Republic of China], although most intrusions focus on exfiltrating data, the skills being demonstrated would also apply to wartime computer network attacks*."[55]

The Chinese military and intelligence services make use of the corporate sector, along with state-owned telecommunication carriers like China Telecom Corporation, for the supply of telecommunications and information technology and services. This fear has culminated in the banning of Huawei, a Chinese telecommunication giant with a worldwide presence, from conducting business in the US on the grounds of its alleged links with the Chinese military. According to some accounts, electronic devices manufactured in China are pre-installed with trojan viruses designed to leak sensitive user information. The Chinese army's cyber-warfare unit has prepared a detailed outline for carrying out IT attacks ranging from network scanning to obtaining passwords and breaking codes, stealing data, information-paralyzing software, information-blocking software, information-deception software & malware, and software for counter-measures. Some of these tactics were used in an IT warfare exercise in the Hubei region in 2000, in which attacks were launched against India, Japan, South Korea, and Taiwan. In another such exercise in the Xian province, new techniques of cyber warfare were practiced that included

> "*planting (dis)information mines; conducting information reconnaissance; changing network data; releasing information bombs; dumping information garbage; releasing clone information; organizing information defense, and establishing network spy stations*".[56]

The PLA cyber warfare specialists created these tactics intending to gain control of India's, Japan's, and Taiwan's communication networks.

[53] Weekly Standard. "Outrage in Berlin Over Chinese Cyber Attacks." 31 August 2007.
[54] Ibid. (Same as 45)
[55] John T. Bennett. "Chinese Buildup of Cyber, Space Tools Worries U.S." Defense News, 13 January 2010.
[56] Ibid. (same as 45)

There are numerous instances of Chinese cyber-attacks against its opponents. For instance, Indian communication and network systems have been a victim of Chinese hackers on several occasions. The INSAT 4B communications satellite from India failed in 2010. The communication satellite ran Siemen's software, which was compromised by the Stuxnet virus. It has been suggested that Chinese hackers disabled the Indian satellite for economic gain, as part of a larger statecraft exercise.[57] According to *Record Future*, a US cybersecurity firm, India's power grid infrastructure is a new target for Chinese hackers. Mumbai was left reeling for hours in October 2020 due to a power outage that interrupted services. According to Recorded Future, the disruption was created by a new alliance of Chinese hackers nicknamed '*Red Echo'*.[58] In 2008, there were accusations that Chinese hackers were frequently attacking the websites and data infrastructure of the National Informatics Centre, the National Security Council, and the Ministry of External Affairs. Cyberattacks increased by more than 200 percent during the Galwan Valley battle between India and China, according to Singapore-based cyber company *Cyfirma*.

Today's conflicts are more technologically centric than they were in the past. In such volatile circumstances, malware serves as weapons, hackers and cybersecurity professionals serve as troops, and the battleground is data. As noted by P.S. Raghavan, India is one of the world's most cyber-targeted countries.[59] To mitigate this persisting cyber threat emanating from China, India is working on developing technology. In 2019, India established the *Defence Cyber Agency* (DCA). DCA serves two functions. It is entrusted with fighting virtual battles in the cyber domain as well as developing a cyber warfare doctrine.[60] As Chief of Defense Staff Bipin Rawat observed,

> "*What we are trying to do is create a system in which we ensure cyber defense. And we have been able to create a cyber agency, which is our agency within the armed forces…*

[57] Peter J. Brown. "Lost Asian Satellites Send Powerful Signals." Asia Times Online, 9 October 2010.
[58] Prabhjote Gill. "The Chinese cyber threat is real — and India's best defence right now is to keep its outage time limited." Business Insider India, 9 April 2021. https://www.businessinsider.in/defense/news/the-chinese-cyber-threat-is-real-and-indias-best-defence-right-now-is-to-keep-its-outage-time-limited/articleshow/81981886.cms., Accessed 24 August 2021.
[59] P.S. Raghavan. "The Evolution of India's National Security Architecture." *Journal of Defence Studies* (Institute for Defence Studies and Analyses) 13, no.3 (2019): 33-52.
[60] Sandeep Dhawan. India-China Cyber Asymmetry: Act Now. Chanakya Forum, 2021. https://chanakyaforum.com/india-china-cyber-asymmetry-act-now/., Accessed 24 August 2021.

Each service also has its cyber agency to ensure that even if we come under a cyber-attack, the downtime and the effect of the cyber-attack does not last long."[61]

Another major concern among the Indian security establishments is the growing market share of Chinese mobile and hardware technology manufacturers in India. India is a leading market for the Chinese mobile industry that offers smartphones at cheaper costs. Chinese tech companies like Xiaomi, Vivo, Oppo, and Realme no doubt dominate the Indian smartphone market. Also, there is an increasing market dominance of Chinese-made network hardware in India. There are speculations that these devices are capable of stealing data and user information.

In cyber warfare, it is not that hard to predict Chinese strategic design against India. Under the project Optical Fibers, Beijing has constructed an optical fiber transmission line in Gansu Province, Qinghai Province, and Tibet Autonomous Region (TAR). This is the first mainline optical cable to be erected in the TAR, and by connecting it to the already constructed main optical fiber transmission lines of Gansu Province, the linking of Qinghai Province, Tibet, and the coastline areas was accomplished. This would provide China with an edge in fighting a "*local war under the conditions of informatization*."[62]

India still has a long way to go in contrast to China's cyber capabilities. For more than two decades, China has been preparing for the fifth dimension of conflict, whereas India, according to Rawat, is still figuring out what it needs to do. This is reflected in the ranking published by the Belfer Center for Science and International Affairs, according to which, India ranked 21st in the National Cyber Power Index and 26th in the Cyber Capability Index.[63]

7. Recent Trends during the Pandemic

People are accessing social platforms such as Instagram, Facebook, Twitter, and others more frequently during the lockdown, in addition to watching movies and series by subscribing to web channels such as Netflix, Amazon Prime, Hot Star, Zee5, and others, and playing online games by installing various applications. In doing so, we tend to grant these apps access to our personal information stored on our phones, computers, and/or social media accounts to log in

[61] Prabhjote Gill. "The Chinese cyber threat is real — and India's best defence right now is to keep its outage time limited".
[62] M.K. Sharma. "Cyber Warfare: Implications for India."
[63] Sandeep Dhawan. India-China Cyber Asymmetry: Act Now. Chanakya Forum.

to the services provided by the apps. Users frequently disclose financial information to acquire applications or access internet services. Furthermore, as a result of the government's "*stay home, stay safe*" campaign, people have grown more reliant on various payment gateways to pay utility bills, and premiums, recharge mobile phones, buy medications and vital commodities online, and engage in other similar online activities. All of these actions have created a breeding ground for malware and ransomware attacks.

Because of the COVID-19 and the mandated lockdown, more individuals are trapped at home, with much more hours to spend online each day and increasingly dependent on the Internet to get services that they would typically receive offline. Cybercrime has existed for many years, but the increase in the percentage of the population connected to the Internet and the amount of time spent online, combined with the sense of confinement, anxiety, and fear generated by the lockdown, has provided more opportunities for cybercriminals to exploit the situation and make more money or cause disruption. This tectonic shift in how we live our lives and utilize the Internet has increased web-based crime.

According to a Kaspersky Security Network (KSN) study, from January to March of this year, its products discovered and blocked 52,820,874 local cyber threats in India.[64] According to data, India is now ranked 27th in the world in terms of the number of web risks detected by businesses in Q1 2020, up from 32nd in Q4 2019. The number of local threats in India in Q1 2020 (52,820,874 threats) demonstrates how frequently people are targeted by malware distributed via portable USB devices, CDs and DVDs, and other methods. According to Lt. Gen. Rajesh Pant, India's National Cyber Security Coordinator (NCSC), cyber thieves have created hundreds of "fraud portals" connected to the coronavirus. These websites have enticed thousands of Indians who want to help combat coronavirus to make donations. Many of these bogus websites are extremely sophisticated, almost indistinguishable from their legitimate counterparts.

8. Cyber-Cooperation with the US & Russia

Despite India being a late entrant to the cyber-security realm, the Indo-US cyber-security coordination has reached a considerable level that was probably inconceivable a decade

[64] The Economic Times. "37% increase in cyberattacks in India in Q1 2020: Report." 25 May 2020. https://ciso.economictimes.indiatimes.com/news/37-increase-in-cyberattacks-in-india-in-q1-2020-report/75962696., Accessed 16 September 2021.

ago. The range of cyber-space issues confronting India and the United States now ranges from national security concerns to the future trajectory of their respective digital economies.[65] Following the visit of former Indian Prime Minister Vajpayee to the United States in 2001, the groundwork for cyber-security cooperation was laid. The visit aided in the formation of the India-US Cyber Security Forum, which stressed "*cyber-security, cyber-forensics, and associated research"* and aims to work *"...towards increasing cooperation among law enforcement authorities on both sides in dealing with cyber-crime*."[66]

This cyber cooperation got pace when the Indo-US strategic dialogue was established in 2010. Building on the foundation established by the bilateral strategic dialogue, New Delhi and Washington signed a memorandum of understanding (MoU) in 2011 to urge increased collaboration and information exchange on cybersecurity.[67] The MoU permits the CERTs of the two countries to share cybersecurity intelligence and work on several other operational and technical issues. The fourth session of the India-US Strategic Dialogue focused on collaboration in cyber-security (2013). Both leaders underlined the need of strengthening cyber-security partnerships, particularly through future iterations of the Cyber Security Consultations, the Strategic Cyber Policy Dialogue, and the Information and Communications Technology Working Group.

Both India and the United States realize that conversations about cybersecurity and the digital economy must take place concurrently rather than separately. India's digital economy is undergoing a historic change as increased Internet use, smartphone use, and entrepreneurial innovation continue to offer up new growth opportunities across the country. A sizable portion of the Indian population is firmly engaged in experiencing a digital ecosystem. Cities and metropolises no longer have a monopoly on the usage of mobile phones, social media, e-commerce, digital payments, and e-governance services; in fact, these services and advancements have effectively penetrated India's vast rural populations. In this regard, the

[65] Samir Saran. "Digital crossroads: Unlocking the potential of India-US cooperation in cyberspace." Orf Issue Briefs and Special Reports (Observer Research Foundation (ORF). 2019. https://www.orfonline.org/research/digital-crossroads-unlocking-the-potential-of-india-us-cooperation-in-cyberspace-56803/., Accessed 7 September 2021.
[66] Rahul Prakash. India-US cyber relations. (New Delhi: Observer Research Foundation, 2014).
[67] Office of the Press Secretary, USA. "United States and India Sign Cybersecurity Agreement." Department of Homeland Security. 19 July 2011. https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement., Accessed September 7, 2021.

United States has emerged as a key player in this ecosystem, with constant investments, technology, and ideas influencing India's digital future.

Despite efforts on both sides to avoid allowing the occasional stumbling block to derail the larger process of greater cyber security cooperation, concerns remain on both sides. The Indian Envoy to the United States, Taranjit Sandhu, says that cyber security is essential for India and the United States' national security, even though both nations have been working technologically for decades. Sandhu stated at the Global Technology Summit,

> "*Technology is helping us in fighting the pandemic today in more ways than one, from staying connected to making trade and commerce easier through digital platforms to facilitating education and healthcare*" however, "*Like any other weapon, it (technology) is prone to misuse too. Therefore, it cannot remain immune from the unpredictability of geopolitics*."[68]

He sees technology and cooperation as the motor and gasoline in India-US ties. Both nations are complementary in the sphere of ICTs and digital space, and their collaboration is critical to both countries' national security.

For decades throughout the Soviet era, India and Russia maintained strong ties at the highest levels. The insecurity of the post-Soviet years, on the other hand, reverberated across the Indo-Russia relationship as the newly created Russian Federation sought to reconstruct its foreign policy. India and Russia both made efforts to restore their ties. In 1993, India and Russia signed the Treaty of Friendship and Cooperation, and a new era of Military-Technical Cooperation began a year later. India would eventually become a significant buyer of Russian weapons. In 2010, to mark the tenth anniversary of the 'Declaration on Strategic Partnership', the leaders of the two countries highlighted the importance of the partnership.

India and Russia inked a broad cyber-security pact on the eve of the BRICS meeting in Goa. The pact is broad in scope, allowing for collaboration not just in combating cybercrime but also in defense and national security. The agreement not only establishes a high-level conversation on cyber problems but also permits government agencies to begin working together on counter-terrorism operations. The cyber pact also appears to reflect both nations' desire to strengthen bilateral ties. The initial push to sign a cyber-security MoU came from

[68] Nayanima Basu. "Cybersecurity is critical for national security of India & US, says Indian envoy to US Sandhu." The Print, 14 December 2020.. https://theprint.in/diplomacy/cybersecurity-is-critical-for-national-security-of-india-us-says-indian-envoy-to-us-sandhu/566765/., Accessed 7 September 2021.

Moscow, but India moved slowly, especially in light of Russia's aggressive push for greater inter-governmental involvement in internet governance issues at the 2015 BRICS summit in the Ufa and Shanghai Cooperation Organization summits. The signing of the US-India cyber framework agreement, on the other hand, left an opportunity for debate because the treaty's basic sections highlighted India's desire for multi-stakeholder participation while keeping a larger government role in security issues. As a result, although ostensibly avoiding allusions to cyber-security, the agreement with Russia is security-heavy, because India interprets the term strictly technically, with no political or economic overtones.

In 2018, Russia and India have confirmed their plans to broaden practical cooperation in cyber security. It was reported, "*…. their intention to expand practical cooperation including the exchange of technological information, to prevent the utilization of IT for criminal, and terrorist purposes.*"[69] The need for countries to establish norms, standards, and principles of responsible cyber conduct within the UN's role as a coordinator was highlighted by Oleg Khramov, Deputy Secretary of the Russian Security Council, and Ajit Doval, India's National Security Adviser. Recognizing the current threats in the field of information technologies and telecommunications, as well as the common approaches to cybersecurity, India and Russia discussed the possibility of establishing a long-term mechanism for cooperation between the two countries' relevant agencies and authorities within the framework of the 2016 intergovernmental agreement on security. In addition, in the aftermath of a cyber-attack on the Kudankulam nuclear power plant established by global nuclear company Rosatom, India, and Russia have increased their efforts to improve cyber security cooperation in 2019.[70]

9. Policy Recommendations

a. The Ministry of Home Affairs should be the nodal agency for dealing with cyberterrorism. A plethora of measures, ranging from monitoring and surveillance to investigation and punishment, will be required to combat cyberterrorism and cybercrime.

[69] TASS. "Russia and India confirm readiness to cooperate in cyber security." Russian News Agency, 17 February 2018. https://tass.com/world/990504., Accessed 17 September 2021.
[70] Dipanjan R. Chaudhury. "India, Russia step up cyber security cooperation after attack on Kudankulam." The Economic Times, 13 November 2019. https://economictimes.indiatimes.com/news/politics-and-nation/india-russia-step-up-cyber-security-cooperation-after-attack-on-kudankulam/articleshow/72033001.cms?from=mdr., Accessed 8 September 2021.

Cyberterrorism should be viewed as an extension of the country's overall counterterrorism capabilities.

b. Cyber security education, research, development, and training will be essential components of the national cyber security plan. The government should establish a well-equipped National Cyber Security R&D Centre to conduct cutting-edge cyber security research and development. The DRDO should undertake specialized research for the military forces, while the NTRO should research the country's intelligence services.

c. International collaboration is critical in dealing with cybercrime, cyberterrorism, and risk management in cyberspace. Participation in multilateral talks on internet behavior standards is required. Indian authorities should also engage in regional cyber security forums. It should be encouraged for Indian cyber authorities to collaborate with internationally recognized cyber professional groups.

d. There is a need to establish a Cyber Command and develop offensive capabilities. A pool of trained individuals, such as Cyber TA Battalions, can also be formed to offer "surge capacity" to the country's resources at crucial moments or in the case of conflicts.

e. Procedural rules must be in place to achieve international organizations' and countries' cooperation and coordination in investigating and prosecuting cybercriminals. The government must make appropriate changes to current laws or adopt new legislation, such as a Data Protection/Privacy Act, to prevent the exploitation of personal information by various government entities and to preserve individual privacy.

10. Conclusion

As a result of the above research, we conclude that India must pursue an offensive cyber warfare policy as a way of strategic balance. This conclusion is founded on the core concept that cyber warfare may cause substantial financial and infrastructure destruction while requiring minimal financing, and it is difficult to identify and fight against. Given India's competence in this sector, an aggressive strategy for cyber warfare is a viable option. By acquiring offensive capabilities, India will be able to reduce, if not eliminate, the risks posed by cyber warfare. ASAT, or Anti-Satellite Technology, is viewed as a new danger to space-based assets. In this regard, India's technological and capacity gap may be filled by using cyber warfare skills until it develops such capabilities. The fundamental goal of our national security strategy is to protect

India's sovereignty and integrity. As a result, our weapons are primarily deployed to protect our borders, rather than to expand our dominion over diverse domains such as land, sea, air space, and cyberspace.[71] While this appears to be reasonable, some argue that the best form of defense is the offense. They think that the capacity to eliminate the opponent by a preemptive strike outweighs the need for a defensive plan.

Increased collaboration and coordination across and within nation-states—among the military services, commercial sector, and academia—is also a critical component of cyber security. Academics already play an important role in cyber security, but their efforts are frequently thwarted by companies and governments because they are viewed as a danger rather than an advantage.[72] This has to change, and the cyber community needs to be more accepting of any study and experimentation that leads to a greater knowledge of cyber vulnerabilities and weaknesses in security systems. The general population is sometimes neglected, yet it may play a vital role in cyber defense. Governments, businesses, and academics would need to exchange data on the most recent assaults, malware signatures, and vulnerabilities.[73]

India’s cyber posturing may be a potent foreign policy instrument. Developed offensive capabilities in cyberspace, unlike traditional military deterrence, do not need to be stored in military formations. India’s strength in IT and IT Enabled Services (ITES) might be used to develop cyber deterrent capabilities to obtain an asymmetric edge over a militarily stronger prospective rival. The synthesis of the National Cyber Security Policy (2013) indicates that the national policy sets lofty goals and encompasses a wide range of activities ranging from an institutional structure for an emergency response to indigenous capacity building. However, a deeper look at NCSP-13 and a thorough study of the cyber organization reveal many flaws in addressing our nation's cyber vulnerabilities. The strategy makes references to CERT-IN and the NCIIPC, but the duties and responsibilities of the armed forces, other government agencies, and the business sector are not clearly stated, leaving the country susceptible to cyber assaults. India has long been recognized as the world’s information backyard; nevertheless, the

[71] M.K. Sharma,. "India’s Cyber Warfare Strategy in Next Decade." Air power (Centre for Air Power Studies) 8, no.3 (2013): 37-66.
[72] Jaikumar Vijayan. Carrier IQ Drops Legal Threat Against Security Researcher. Computerworld. (2011).
[73] Jason Healey. "Cybersecurity Legislation Should Force U.S. Government to Listen Less and Speak More." The Atlantic, 15 March 2012.

government's attempts to address cyber security over the previous two decades have been reactive and fragmented.

If India is to remain relevant in today's security climate, it must accept cyberwarfare as one of the most significant elements in the outcome of future battles. Future wars will be increasingly network-centric, allowing for a power shift away from kinetic weapons and toward non-kinetic weaponry. Because of its unique character and function in society, cyberwarfare as a subset of information warfare would have a lion's share in planning and conducting future conflicts all over the world.

References

Ball, Desmond. "China's Cyber Warfare Capabilities." *Security Challenges* 7, no.2 (2011): 81-103.

Basu, Nayanima. "Cybersecurity is critical for the national security of India & US, says Indian envoy to US Sandhu." The Print, 14 December 2020.. https://theprint.in/diplomacy/cybersecurity-is-critical-for-national-security-of-india-us-says-indian-envoy-to-us-sandhu/566765/., Accessed 7 September 2021.

Bennett, John T. "Chinese Buildup of Cyber, Space Tools Worries U.S." Defense News, 13 January 2010.

Brenner, Susan W. Cybercrime metrics: old wine, new bottles? *Virginia Journal Oflaw & Technology* 9, no.13 (2014): 1-52.

Brown, Peter J. "Lost Asian Satellites Send Powerful Signals." *Asia Times Online*, 9 October 2010.

Bureau, ET. "Government Mulls Digital India Programme to Connect All Villages." *The Economic Times*, 21 August 2014, https://economictimes.indiatimes.com/news/economy/policy/government-mulls-digital-india-programme-to-connect-all-villages/articleshow/40524106.cms. Accessed 02 September 2021.

Buzan, Barry. *People, States, and Fear: An Agenda for International Security Studies in the Post Cold War Era*. (London: Harvester Wheatsheaf, 1991).

Centre of Excellence Defence Against Terror, NATO Science for Peace and Security, (IOS Press; 1st ed., 2008)

Chaudhury, Dipanjan R. "India, Russia step up cyber security cooperation after the attack on Kudankulam." *The Economic Times*, 13 November 2019. https://economictimes.indiatimes.com/news/politics-and-nation/india-russia-step-up-cyber-security-cooperation-after-attack-on-kudankulam/articleshow/72033001.cms?from=mdr., Accessed 8 September 2021.

Chertoff, Michael and Paul Rosenzweig. "*A Primer on Globally Harmonizing Internet Jurisdiction and Regulations*." (2015).

China Review News. "The People's Liberation Army's First Force on Strategic Information Support and Protection is Established." 20 July 2010.

Debarati, Halder. Information Technology Act and Cyber Terrorism: A Critical Review (August 1, 2011). Available at SSRN: https://ssrn.com/abstract=1964261 or

http://dx.doi.org/10.2139/ssrn.1964261

Dhawan, Sandeep. India-China Cyber Asymmetry: Act Now. Chanakya Forum, 2021. https://chanakyaforum.com/india-china-cyber-asymmetry-act-now/., Accessed 24 August 2021.

DIETY. Discussion Draft on National Cyber Security Policy, (New Delhi: Government of India, 2011).

Dutta, Sanjay. "10 power assets, Mumbai, Tamil Nadu ports came under RedEcho cyberattack." *The Times of India*, March 2021. https://timesofindia.indiatimes.com/business/india-business/10-power-assets-mumbai-tamil-nadu-ports-came-under-redecho-cyberattack/articleshow/81337328.cms., Accessed 6 September 2021.

Gercke, Marco. *Understanding Cybercrime: A Guide for Developing Countries*, (Geneva: ITU Publication, 2009)

Ghate, S. Shweta and Pragyesh Kumar Agrawal. "A Literature Review on Cyber Security in Indian Context", *Journal of Computer & Information Technology* 8, no.5 (2017): 30-36.

Gill, Prabhjote. "The Chinese cyber threat is real — and India's best defense right now is to keep its outage time-limited." *Business Insider India*, 9 April 2021. https://www.businessinsider.in/defense/news/the-chinese-cyber-threat-is-real-and-indias-best-defence-right-now-is-to-keep-its-outage-time-limited/articleshow/81981886.cms., Accessed 24 August 2021.

Halder Debarati, *Information Technology Act and Cyber Terrorism: A Critical Review* (August 1, 2011). Available at SSRN: https://ssrn.com/abstract=1964261 or http://dx.doi.org/10.2139/ssrn.1964261

Healey, Jason. "Cybersecurity Legislation Should Force U.S. Government to Listen Less and Speak More." *The Atlantic*, 15 March 2012.

Jain, S. "Cyber Security: A Sine Qua Non.", (2014), http://www.indiandefencereview.com/news/cyber-security-a-sine-qua-non/., Accessed 2 September 2021.

Joseph, Josy. "India to Add Muscle to Its Cyber Arsenal." *The Times of India*, 11 June 2012.

Kaul, Ayushman, and Khalid Shah. "Indian government's 2G restrictions in Kashmir fail to curb online extremism." *DFR Lab*. 25 May 2020. https://medium.com/dfrlab/indian-governments-2g-restrictions-in-kashmir-fail-to-curb-online-extremism-ea7a461f71cd., Accessed September 11, 2021.

Kaushik, R.K. "Cyber Security Needs Urgent Attention of Indian Government.", 2014. http://cybersecurityforindia.blogspot.in/2014/09/cyber-security-needs-urgent-attention.html, Accessed September 2, 2021.

Kumar, V. Ananda, Krishan K. Pandey, and Devendra Kumar Punia. *Facing the Reality of Cyber-Threats in the Power Sector*. (Bangalore: Wipro Technologies, 2013).

Liu, Shuran, Su Guo and Hui Deng. "Analyses and Discussions of the Blackout in Indian Power Grid." *Energy Science and Technology* 6, no.1 (2013): 61-66.

Miller, Greg and Souad Mekhennet. "Inside the surreal world of the Islamic State's propaganda machine." *The Washington Post*, 20 November 2015. https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92ddd2b_story.html., Accessed 30 August 2021.

Mint. 2021. "Centre says four load despatch units came under cyberattack." July 22. https://www.livemint.com/news/india/indias-four-regional-load-despatch-centres-faced-cyberattacks-govt-11626856955565.html., Accessed September 5, 2021.

MP-IDSA. India's Cyber Security Challenges. (New Delhi, 2012). https://idsa.in/system/files/book/book_indiacybersecurity.pdf, Accessed 1 September 2021.

Mr. Srijit Banerjee was interviewed by the author on 26th August 2021.

Mustafa, Ghulam, Zainab Murtaza and Khadija Murtaza. "Cyber Warfare between Pakistan and India: Implications for the Region." *Pakistan Languages and Humanities Review* 4, no.1(2020): 59-71. DOI:10.47205/plhr.2020(4-I)2.5.

Naik, Saheli. "A Biggest Threat to India – Cyber Terrorism and Crime." *Journal of Research in Humanities and Social Science* 27, (2017): 27-30.

Nanda, Prashant K. "Cyberattacks surged 3-fold to 1.16 mn last year in India." Mint,23 March 2021. https://www.livemint.com/news/india/as-tech-adoption-grew-india-faced-11-58-lakh-cyberattacks-in-2020-11616492755651.html., Accessed 2 September 2021.

News Desk. "Pakistani hackers attacked 2,118 Indian websites." 2014. *Pakistan Todays*.

Office of the Press Secretary, USA. "United States and India Sign Cybersecurity Agreement." Department of Homeland Security. 19 July 2011. https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement., Accessed 7 September 2021.

Oh, Onook, Manish Agrawal, and H. Raghav Rao. "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter." *Information Systems Frontiers* 13, no.1 (2011): 33-43.

Pandit, Rajat. "Army gearing up for cyber warfare." The Times of India, 7 July 2005, https://timesofindia.indiatimes.com/india/army-gearing-up-for-cyber-warfare/articleshow/1163080.cms., Accessed 02 September 2021.

Parmar, Sushma Devi. "Cybersecurity in India: An Evolving Concern for National Security." *The Journal of Intelligence and Cyber Security* 1, no.1 (2018).

Prakash, Rahul. *India-US cyber relations*, (New Delhi: Observer Research Foundation, 2014).

Pujari. Amaresh. *Cyber Terrorism: World Wide Weaponisation*! Tamil Nadu Police Sesquicentennial Anniversary Souvenir, (2017).

Raghavan, P.S. "The Evolution of India's National Security Architecture." *Journal of Defence Studies* (Institute for Defence Studies and Analyses) 13, no.3 (2019): 33-52.

Raman, Shiv, and Nidhi Sharma. "Cyber Terrorism in India: A Physical Reality or Virtual Myth." *Indian Journal of Law and Human Behavior* 5, no.2 (2019): 133-140. Doi: http://dx.doi.org/10.21088/ijlhb.2454.7107.5219.5.

Rather, Mohd Aarif and Kishor Jose. "Human Security: Evolution and Conceptualization." *European Academic Research* 2, no.5 (2014): 6766–6797.

Saran, Samir. "Digital crossroads: Unlocking the potential of India-US cooperation in cyberspace." Orf Issue Briefs and Special Reports (Observer Research Foundation (ORF). 2019. https://www.orfonline.org/research/digital-crossroads-unlocking-the-potential-of-india-us-cooperation-in-cyberspace-56803/., Accessed 7 September 2021.

Sharma, M.K. "Cyber Warfare: Implications for India." *In India's National Security Annual review 2011*, ed. *Satish Kumar*, (Routledge: 2011).

Sharma, M.K. "India's Cyber Warfare Strategy In Next Decade." *Airpower* (Centre for Air Power Studies) 8, no.3 (2013): 37-66.

Sherman, Jason. "Report: China Developing Force to Tackle Information Warfare." *Defense News*, 27 November 2000.

Singh, Harsimran and Joji Thomas Philip. "Spy Game: India Readies Cyber Army to Hack into Hostile Nations Computer Systems." The Economic Times, 06 August 2010, https://economictimes.indiatimes.com/spy-game-india-readies-cyber-army-to-hack-into-hostile-nations-computer-systems/articleshow/6258977.cms?from=mdr., Accessed 02 September 2021.

Taneja, Kabir. *From 4G to Languages: The Developing Online Jihadist Propaganda Network in India.* (New Delhi: Observer Research Foundation, 2020).

TASS. "Russia and India confirm readiness to cooperate in cyber security." Russian News Agency, 17 February 2018. https://tass.com/world/990504., Accessed 17 September 2021.

The Economic Times. "37% increase in cyberattacks in India in Q1 2020: Report." 25 May 2020. https://ciso.economictimes.indiatimes.com/news/37-increase-in-cyberattacks-in-india-in-q1-2020-report/75962696., Accessed 16 September 2021.

UNIDIR. *The Cyber Index: International Security Trends and Realities*, (New York and Geneva: United Nations Institute for Disarmament Research, 2013).

Van Slyke, Shanna and Michael L. Benson, *The Oxford Handbook of White Collar Crime*, (Oxford University Press, 2016).

Vijayan, Jaikumar. *Carrier IQ Drops Legal Threat Against Security Researcher*, (Computerworld, 2011).

Walstrom, Michael. *India's Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges*. (Seattle: Henry M. Jackson School of International Studies, 2016).

Weekly Standard. "Outrage in Berlin Over Chinese Cyber Attacks." 31 August 2007.

Weimann, Gabriel. *Cyberterrorism: How Real Is the Threat?* (Washington D.C.: United States Institute Of Peace, 2004). www.usip.org., Accessed 1 September 2021.