Indian J. Soc. & Pol. 12 (02):39-46: 2025
31 JULY 2025

ISSN: 2348-0084 (PRINT)
ISSN: 2455-2127(ONLINE)

CYBERWARFARE: EMERGING SECURITY THREAT IN THE 21ST CENTURY AND INDIA'S PREPAREDNESS

MANORAMA KUNTAL[1]

[1]Research Scholar, Affiliation and Institution: Department of Political Science, Jamia Millia Islamia, New Delhi

ABSTRACT

The 21st century has significantly increased the risk of cyber warfare and other cyber threats. The rapid expansion of Internet use has increased vulnerabilities, exposing individuals and systems to unprecedented risks. The Internet and wireless communications are crucial to economic, social, political, and military operations across all domains: land, sea, air, and space. Unlike traditional warfare, cyber warfare operates in its own independent theatre, i.e. cyber space recognized as the fifth domain of warfare after land, air, sea, and space. This domain's infrastructure relies on physical assets, such as microwave links, telecom exchanges, undersea cables, and routers, all of which are safeguarded by traditional military forces. This paper examines cyber warfare as a critical and emerging non-traditional security threat of the 21st century—one that is inherently transnational and unconstrained by geographical boundaries. This paper utilizes both primary and secondary sources to emphasize the importance of understanding cyber warfare and its associated cyber threats, as well as their impact on India's economy and infrastructure. Furthermore, the paper evaluates India's readiness to address various cyber threats, underscoring the need for robust cybersecurity measures and strategic preparedness in response to this evolving global challenge.

KEYWORDS: *Cybersecurity, Cyberwarfare, Security, 21st Century, India*

INTRODUCTION

There has been a shift in security discourse post the end of Cold War, whereby the focus has been shifted to non-traditional security threats, namely climate change, poverty, cyberwarfare, infectious disease etc. (Buzan, Waever, & Wilde, 1998) The end of the Cold War put military considerations to the margins, making way for the larger security agenda to take centre stage (Buzan & Hansen, 2009) Similarly, with the advancement of technology there has been an increased use of cyberspace, encompassing computers, smartphones, and the Internet, which has concurrently increased cyber threats .Cyber power is becoming a crucial tool in shaping and implementing national policies, including counter-terrorism, economic development, and diplomacy. The US–China rivalry in the region pressures India to strengthen its power to protect its sovereignty, ensure territorial integrity, and contribute to global stability while fostering economic growth and addressing domestic disparities. Cyber power can enhance and integrate with other national power elements, creating a synergistic effect that strengthens overall national capabilities. (Sharma, 2013) Information Technology has revolutionized global connectivity and economic development but also introduced significant vulnerabilities. Information Technology (IT) significantly impacts infrastructure such as telecommunications, transportation, and defence systems. Cybersecurity threats, originating from various sources, impact individuals, businesses, and national infrastructure, posing severe risks to public safety, national security, and economic stability. Identifying the origin and motivation of these threats is often challenging (Lok Sabha Secretariat, 2017) The rise in cyber threats necessitates robust cybersecurity measures due to their multifaceted nature. Cyber threats, including cyber warfare and cyberterrorism, threaten national security, with crimes categorized into two main groups: those targeting computer systems directly (e.g., viruses, malware) and those facilitated by computer networks (e.g., economic fraud, phishing). Prominent threats include hacking and identity theft, particularly concerning for India. (Bhattacharya, Ray, Sinha, & Sachdev, 2021) Therefore, Sharma emphasized on the importance of developing a cyber strategy (Sharma, 2013) Cyber strategy means development and employment of strategic capability to operate in cyber space, integrated and coordinated with the other operational domains (land, sea, air and outer space) (Sharma, 2013) The global internet space, not under the jurisdiction of any single country, necessitates national cooperation and robust defence security to protect a nation's cyber space. (Bhattacharya, Ray, Sinha, & Sachdev, 2021)This paper aims to understand cyberwarfare as an emerging non-traditional security threat, instances of cyberattacks and their impact. The paper also discusses India's preparedness to tackle with these cyberattacks.

1: Corresponding Author

UNDERSTANDING CYBERWARFARE

Although there has been a debate on how to define Cyber warfare but it is generally defined as a series of cyberattacks by one nation-state against another using the internet as a weapon, with the potential to disrupt vital systems or even cause loss of life. This includes attacking critical infrastructure and strategic controls, hacking important websites, and gathering intelligence. Cyber warfare is practiced by states, individual organizations, and terrorist groups, often referred to as cyber terror. (Bhattacharya, Ray, Sinha, & Sachdev, 2021)

According to the Cybersecurity and Infrastructure Security Agency, the goal of cyberwarfare is to "weaken, disrupt or destroy" another nation. (Gillis, 2023) Cyberwarfare is a strategic competition in cyberspace, allowing countries to conduct large-scale, covert, inexpensive, and anonymous operations. It spans economic, societal, cultural/intellectual, military, and political domains. Heavily internet-reliant countries face significant threats, from IP theft to attacks on small businesses and critical infrastructure like the electricity grid. Cyberwarfare is cost-effective and hard to trace, requiring only motivated individuals with basic resources. (Miller & Kirda, 2020) Cyber warfare can present various threats towards a nation. At the most basic level, cyber-attacks can be used to support traditional warfare. Unlike traditional warfare, cyber warfare operates in an independent theatre of war. The internet and wireless communications play vital roles in economic, social, political, and military operations across land, sea, air, and space. Cyber space is considered the fifth domain of warfare, following land, air, space, and sea. Cyber space is unique as it lacks defined boundaries like those of land, sea, and air forces. Its infrastructure depends on physical assets like microwave links, telecom exchanges, undersea cables, and routers, protected by traditional military arms. (Bhattacharya, Ray, Sinha, & Sachdev, 2021)

Robinson (Robinson, Jones, & Janicke, 2015) proposed a definitional model to distinguish cyber warfare attacks from other cyber-attacks without military intent, focusing on the intent and the actor behind the attack. The model effectively identifies simple attacks using an algorithm with if-else conditions. However, accurately determining the true intent of an attack requires understanding the actor's motivation. For a comprehensive detection of cyber warfare, a multidisciplinary approach that integrates technical, legal, military, and political aspects is necessary. (Robinson, Jones, & Janicke, 2015)

The history of cyberwarfare can be traced back to a notable cyberattack occurred in 2010 with the "Stuxnet" malware, designed to sabotage Iran's nuclear facilities by simulating internal engineering failures. (Fortinet, n.d.) This sophisticated attack, reportedly a US-Israeli collaboration, demonstrated how governments could use malware for covert objectives. However, malware creation doesn't always need government collaboration. Individuals, often encouraged by their governments, can launch attacks. (Fortinet, n.d.) For instance, China's collaboration between the People's Liberation Army and universities to train hackers is well-documented. Due to the anonymity of cyberattacks, perpetrators often face no real consequences. (Miller & Kirda, 2020). In 2013 US conducted Cyber espionage against countries like Brazil and Germany and uncovered through Edward Snowden's leaked documents. In 2014, a North Korean state-affiliated hacking group infiltrated Sony Pictures Entertainment, leaking sensitive documents in retaliation for "The Interview," a film depicting North Korea negatively. (Fortinet, n.d.)

Between 2014 and 2016, Russia conducted strategic cyberattacks targeting Ukraine and the German parliament. Concurrently, China executed a cyber espionage operation, compromising 21.5 million personnel records from the U.S. Office of Personnel Management. In 2017, the WannaCry ransomware attack targeted over 200,000 Windows computers across 150 countries. Subsequently, the NotPetya malware, which first emerged in Ukraine, caused extensive file destruction and inflicted damages exceeding $10 billion. (Fortinet, n.d.) Other incidents include China's 2015 U.S. personnel data theft, Russia's 2016 U.S. election interference, China's 2018 intellectual property theft, the 2019 U.S. cyber-attack on Iran, and the ongoing Russian cyber-attacks on Ukraine has seen a surge in digital warfare, including the deployment of wiper malware extensively targeting Ukrainian organizations amidst the ongoing physical conflict. (Gillis, 2023)

METHODS AND IMPACT OF CYBERWARFARE

Cybersecurity threats arise from a diverse range of sources and manifest in various forms, each targeting different objectives, ranging from malware like viruses and ransomware to disrupt or hold critical infrastructure hostage, to DDoS attacks aimed at overwhelming networks. (Gillis, 2023) **Cyber terrorism** involves premeditated disruptive actions or threats against computer systems to advance social, ideological, or political goals, or to intimidate individuals. **Cyber fraud** focuses on financial gain through tactics such as phishing and fake websites, which steal personal details and funds. **Cyber spying** aims to gather sensitive information, often for sale or exploitation. Espionage through techniques like phishing and spyware is used for intelligence gathering, while subversive efforts involve digital propaganda to destabilize societies.

(Buxton, 2023) **Cyber stalking or bullying** seeks to intimidate individuals, usually through social media platforms like Facebook or Twitter. Lastly, **cyber assault** targets the damage or destruction of information or equipment, including physical harm to systems or deletion of critical data. (Sethi & Thakur, 2017) Insider threats also pose significant risks, often aiding external adversaries. These activities are executed by state-affiliated groups to protect national interests or undermine other states (Gillis, 2023) (Buxton, 2023)

Cyber-attacks primarily involve internet-based conflicts driven by political motives, targeting information and information systems. (Sethi & Thakur, 2017) Such threats pose significant risks to public safety, national security, and the stability of the interconnected global economy. As nations' critical systems become more interconnected, the risk of cyberwarfare increases. (Gillis, 2023) Attacks can include data theft, destabilization of critical infrastructure like power grids, economic disruption through bank and stock market networks, propaganda to undermine public trust, and sabotage of government systems. State-sponsored attacks often aim to acquire sensitive military intelligence. (Gillis, 2023)These attacks can also compromise the functionality of official websites and networks, disrupt or disable critical services, steal or modify sensitive data, and severely impact financial systems, among other potential consequences. (Sethi & Thakur, 2017) The overarching aim of such cyber-attacks is often to destabilize or undermine the targeted entity's operations and security. (Sethi & Thakur, 2017) Cyber warfare can also significantly impact individuals through identity theft, financial loss, and physical harm due to disruptions to essential infrastructure and services. (Gillis, 2023) More broadly, coordinated cyberattacks can create chaos, erode public trust, and potentially incite civil unrest and political instability. (Buxton, 2023) For instance, from 2016 to 2018, India faced significant cyberattacks, including WannaCry, Petya, and Aadhaar breaches, leading to substantial financial losses. **Mumbai Blackouts (2020)** which was Believed to be a Chinese cyberattack serving as a warning to India, resulting in widespread power outages. The origins of these disruptions, the identities of the perpetrators, and their motivations are often challenging to determine, as attacks can be launched from virtually anywhere. These characteristics make information technology a potent tool for disruptive activities. Currently, cybersecurity threats represent one of the most critical challenges to economic stability and national security. (Sethi & Thakur, 2017)

ASSESSING INDIA'S PERPAREDNESS

India ranks second globally in the number of internet users after China. (World Population Review, 2024) However, its cybersecurity framework is still in the early stages of development. (Bhattacharya, Ray, Sinha, & Sachdev, 2021) Cyber threats are rapidly escalating on a global scale. According to the recent study by PRAHAR (Public Response against Helplessness and Action for Redressal), a not-for-profit organization, cyberattacks on India are projected to rise to an alarming rate of 1 trillion per annum by 2033, reaching 17 trillion by 2047, when the country turns 100. (Saraswat, 2024) Similarly, according to Data Security Council of India(DSCI)'s report, India had detected an average of 761 cyberattack attempts per minute in the year 2024 alone, with the healthcare industry being the top target sector. (Saraswat, 2024). Such revelations constantly set the reminder to focus on guarding against the rising cyber-attacks in the 21st century.

The power outage in Mumbai in October 2020 sparked significant debate over whether it was the result of a cyberattack, with conflicting statements from the Maharashtra and Union governments. Regardless of whether Chinese state-sponsored hackers were responsible for the five-hour power failure, the incident highlighted the vulnerability of India's critical infrastructure. A similar concern arose in October 2019 when the Kudankulam Nuclear Power Plant was targeted by malware, although the plant's operations remained unaffected. (Hooda, 2021) Apps leaking data without security have exacerbated cyber terror. In 2019, India faced 40,000 cyber-attacks from China targeting the IT and banking sectors. (Bhattacharya, Ray, Sinha, & Sachdev, 2021)

During the lockdown, cyber-crime cases surged dramatically, with two months' worth of cases equalling those reported over the past decade. Since the 2000s, technological advances have fuelled a rise in global cyber warfare, impacting economies and targeting major banks and national data. India has also faced instances of cyber terrorism in recent years. (Bhattacharya, Ray, Sinha, & Sachdev, 2021) Zoom, widely used by companies and institutions for classes and meetings, lacked security, leading to data leaks from governments and organizations, posing a national threat. Cyber forensics can help mitigate cyber warfare in several ways. (Bhattacharya, Ray, Sinha, & Sachdev, 2021)

EXISTING CYBER SECURITY INFRASTRUCTURE IN INDIA

In India, cyber safety is primarily managed by government agencies like CERT-In. However, with the rapid evolution of cyber threats, it is essential to engage private actors through a Public-Private Partnership (PPP) model to effectively combat cybercrimes. (Bhattacharya, Ray, Sinha, & Sachdev, 2021)

In 2013, India established a national policy on cyber security, forming the National Critical Information Infrastructure Protection Centre (NCCIPC) to safeguard critical systems with a verified firewall. The National Cyber Collaboration Centre was also created to report on cyber threats and share information with key stakeholders. The Indian Statistical Institute in Kolkata established a Centre of Excellence in Cryptology. A collaborative roadmap on cyber security was developed between the government and the private sector, and CERT-In (Computer Emergency Response Team-India) was established to handle specific incidents. The army, railway, and power sectors also created their own CERTs. A cyber crisis management plan was implemented with state governments to address cyber threats and terrorism. The National Cyber Safeguard Coordination (NCSC) under the National Security Council Secretariat coordinates cyber safety efforts nationally. In 2018, the Cyber Surakshit Bharat Initiative was launched to raise awareness about cyber-crime and train Chief Information Security Officers (CISOs) and IT staff across government agencies. The Information Security Education and Awareness Project (ISEA) was formed to promote education, research, and training in data security. (Bhattacharya, Ray, Sinha, & Sachdev, 2021) Multiple agencies share data daily to combat cyber threats, and the government has signed pacts with neighbouring and other countries for data protection. However, India's poor cyber infrastructure needs development through training and courses to increase public awareness of cyber threats. Cybercrime, a new form of weapon less warfare, has surged since the 2019 lockdown, with a cyber-crime reported every five minutes. (Bhattacharya, Ray, Sinha, & Sachdev, 2021) To combat cybercrime, the National Cybercrime Reporting Portal (https://cybercrime.gov.in) was launched in 2018, allowing citizens to report various cybercrimes, particularly those targeting women and children. Managed by State/UT Law Enforcement Agencies, it ensures legal action. (Chadha, 2024) Since its inception, over 2.3 million incidents have been reported, leading to the registration of more than 45,700 FIRs. The Budapest Convention is the first international agreement addressing internet and cyber-crimes, focusing on harmonizing laws, enhancing investigations, and fostering international collaboration. While it offers significant protection against cyber-crimes, India is not a participant, citing concerns that cross-border data access may infringe on national sovereignty. (Bhattacharya, Ray, Sinha, & Sachdev, 2021)

Additionally, the National Cyber Forensic Laboratory (NCFL) was established in 2019 to provide forensic support to law enforcement agencies (LEAs) and has since assisted in approximately 7,800 cases. The NCFL also offers advanced training to state LEAs, equipping over 600 personnel in digital investigation and cyber forensics, reflecting India's commitment to strengthening its cyber defence and response capabilities. (STANDING COMMITTEE ON FINANCE, 2022-2023) Apart from this, The 'Citizen Financial Cyber Fraud Reporting System' under I4C has saved over ₹1200 crore from financial frauds. CERT-In, in collaboration with RBI, conducts audits and awareness campaigns to enhance cybersecurity and prevent financial fraud. (Chadha, 2024)

Governments and prominent organizations invest in sophisticated cybersecurity measures, such as antivirus software, VPNs, and data encryption, supported by specialized teams. Proactive practices, like penetration testing and ethical hacking, reveal vulnerabilities. Programs like the U.S. "Hack the Pentagon" engage freelance hackers in a crowdsourced approach, adopted by similar agencies globally. (Buxton, 2023)

CHALLENGES PERSIST DESPITE THE EXISTING INFRASTRUCTURE

There are various reasons which can be attributed to the surge in cyberattacks in India. For instance ,geopolitical tensions, rapid digitization, and low cyber awareness are amongst the many. (Saraswat, 2024) Countries like China and Pakistan, are targeting critical infrastructure and sensitive data. The shift from physical to digital warfare has made cyber espionage a key threat. Easier access to hacking tools, AI-powered cyber threats, and widespread internet adoption have increased vulnerabilities towards these cyber threats. As Dr. Sushil Meher notes, even minimal resources like a laptop, an internet connection, and access to open-source tools can enable cyberattacks. (Saraswat, 2024) additionally,Major Kumar mentions that low digital literacy and sophisticated cyber tactics make individuals and organizations the easy targets for such attacks. (Saraswat, 2024)

Ebert (Elbert, 2020) explored the rise of cyber threats to India's national security over the past two decades, pointing out gaps between cybersecurity legislation and its implementation due to political constraints and a lack of multistakeholder cooperation. Although India's cyber diplomacy is advanced, its practical application remains limited, weakening its cyber defence. A more decentralized approach involving government, citizens, and technical teams is needed to strengthen cyber defences, especially since adversaries often target less-secured private and non-governmental sectors. (Elbert, 2020)

The Department of Electronics & Information Technology (DeitY) identifies several critical cyber security challenges within the digital realm. India's cyber space remains inadequately protected due to insufficient ICT infrastructure˙ (Bhattacharya, Ray, Sinha, & Sachdev, 2021) Key issues include a shortage of skilled personnel, such as auditors and IT experts, and insufficient infrastructure and research and development to secure cyberspace. Budget constraints and threats from foreign-hosted servers exacerbate the problem, alongside concerns regarding imported electronic and IT products. Emerging technologies like cloud computing, big data, and the Internet of Things (IoT) add complexity. Balancing cyber security with privacy rights, managing the expanding IT sector, and addressing rapid changes in security threats further complicate the landscape. Additionally, difficulties in tracing attack origins and ensuring adherence to laws in a borderless environment present ongoing challenges. (Standing Committee of Information and Technology, 2013-14)

India lacks a robust cyber security infrastructure despite the 2013 policy INTRODUCTION due to limited awareness and knowledge of cyber threats among individuals and businesses, coupled with inadequate resources to effectively address these issues, with many policies yet to be implemented (Bhattacharya, Ray, Sinha, & Sachdev, 2021) Key vulnerable areas include defence installations, air traffic control management, financial services, railway traffic control, communication networks (including satellites), and sensitive data related to internal and external security, as well as premier institutions of science, technology, and research. (Saluja, 2023)Key issues include the increase in cyber-attacks on Indian businesses, government-led cybersecurity initiatives, and private sector efforts to strengthen cybersecurity. Major threats remain malware, viruses, phishing attacks, and broader cyber-attacks. (Saluja, 2023) Phishing, involving deceptive emails or websites to steal personal information, has seen an uptick, as evidenced by the 2017 attack on the Reserve Bank of India that resulted in a $1 million loss. Malware and ransomware also pose significant threats, with incidents like the 2016 WannaCry attack impacting organizations such as the Andhra Pradesh police force and BSNL. (Saluja, 2023) However, there are positive developments as both the government and private sector increasingly prioritize cybersecurity through awareness initiatives and improved practices like two-factor authentication, data encryption, and regular data backups. (Saluja, 2023)

Challenges in cyberspace are multifaceted, involving the misuse of the internet, social media, technological gaps, and legal obstacles. Criminals exploit digital tools to commit a range of cybercrimes, such as financial fraud, ransomware, identity theft, and privacy breaches. The extensive use of cyberspace, particularly during the COVID-19 pandemic, has increased the vulnerability of citizens, including women and children, to online harassment, stalking, and other cybercrimes. Social media platforms, due to their anonymity and global reach, are often misused to spread fake news and misinformation, complicating law enforcement efforts. Additionally, low cyber literacy and insufficient training of law enforcement agencies (LEAs) hinder the effective management of cybercrimes, which are often facilitated by sophisticated technologies like malware, botnets, and encryption, that provide anonymity and obfuscation. The legal framework, primarily the Information Technology Act of 2000, struggles with challenges such as the transnational nature of cybercrimes, jurisdictional complexities, and difficulties in tracing cybercriminals due to the lack of harmonized international legislation and the presence of data centres outside national boundaries. These factors collectively impede effective cybercrime attribution and prosecution. (STANDING COMMITTEE ON FINANCE, 2022-2023)

Recent Digital Personal Data Protection Act 2023 aims to safeguard both public and private sectors from cyber-attacks but has faced criticism for potentially limiting innovation and not fully ensuring privacy due to the broad powers granted to the Central Government (Meity, 2023) . Despite these efforts, India continues to face frequent cyber-attacks, underscoring the need for stronger cybersecurity measures.

STEPS TOWARDS CYBERSECURITY

In India, the rising incidence of cyber-attacks on businesses and government institutions has elevated cybersecurity to a national priority. Cybersecurity involves safeguarding electronic information from unauthorized access or theft by preventing, detecting, and responding to attacks on networks, systems, and data· (Saluja, 2023) To enhance cyber security, the Government of India has identified a list of critical computer infrastructures requiring protection against cybercrime. This list includes networks related to defence, banking, stock markets, the power grid, national security, railways, airlines, and weather systems. (Bhattacharya, Ray, Sinha, & Sachdev, 2021)

The National Security Council Secretariat (NSCS) in India proposed a Framework for Enhancing Cyber Security which assigned various responsibilities to different ministries and agencies to secure Indian cyberspace. The Ministry of Home Affairs (MHA) was tasked with developing policies for the classification, handling, and security of government information, leading to the issuance of the National Information Security Policy and Guidelines (NISPG) in 2014 and an updated version in 2019. To address specific cybersecurity challenges, additional roles were allocated to various departments over time. For example, the National Critical Information Infrastructure Protection Centre (NCIIPC) was established in 2017 under the Information Technology Act, 2000, to protect critical information infrastructure. The Ministry of Electronics and Information Technology (MeitY) is responsible for developing cyberspace policies and manages agencies like the Computer Emergency Response Team (CERT-In), which coordinates responses to cybersecurity incidents, and the National Cyber Coordination Centre (NCCC), operational since 2017, which monitors internet traffic data for national security. Regular coordination meetings on cybersecurity are held by the MHA to align efforts across multiple departments. (STANDING COMMITTEE ON FINANCE, 2022-2023) Concurrently, the private sector is enhancing cybersecurity measures through the creation of Security Operations Centres (SOCs) and the adoption of advanced cybersecurity technologies (Saluja, 2023)

The Ministry of Electronics and Information Technology has also implemented several measures to enhance cybersecurity for citizens. CERT-In, as part of its services, promotes awareness through initiatives like Cyber Security Awareness Month, Safer Internet Day, and Cyber Jagrookta Diwas. These events are aimed at educating both citizens and the technical community about cybersecurity practices. Additionally, the Cyber Swachhta Kendra (CSK) has been established to detect and mitigate botnet infections, covering 94% of Indian internet users and 755 organizations. CERT-In also provides security tips on its website to help users protect their digital devices and prevent cyber threats like phishing. (STANDING COMMITTEE ON FINANCE, 2022-2023)

International collaboration on cyber security has seen significant advancements involving India. Under the U.S.-India Cyber Relationship Framework, both nations committed to sharing best practices, real-time threat information, and fostering cooperation between law enforcement and research sectors to enhance cyber security and protect internet infrastructure. Similarly, in 2015, India and the U.K. agreed to collaborate on cyber security by establishing a Cyber Security Training Centre of Excellence and supporting the creation of India's National Cyber Crime Coordination Centre. India also engages in cyber security partnerships with the European Union and Malaysia. Additionally, a 2015 Memorandum of Understanding (MoU) with Japan, through CERT-In and Japan-CERT, facilitates the exchange of information on threats, vulnerabilities, and mitigation strategies. (Standing Committee of Information and Technology, 2013-14)

Sharma (Sharma, 2013)emphasized the need for a comprehensive cyber warfare strategy in India that integrates strategic, operational, and tactical dimensions. Despite this, India's offensive cyber capabilities lag behind those of other nations due to a focus on cyber deterrence rather than offense. There is a need for simultaneous development of cyber infrastructure and training. Similarly, Kumar and Mukherjee (Kumar & Mukherjee, 2013) [7] highlighted the urgent need for cybersecurity experts and proposed initiatives like cyber hubs and a cyber literacy framework, which have not been fully implemented. Globally, evolving military doctrines underscore the importance of establishing dedicated cyber commands, highlighting a strategic pivot towards strengthening deterrence in cyberspace. (Sharma, 2013)

Though not primary targets, individuals can be affected by cyber warfare, facing service disruptions and data breaches. To safeguard personal devices, utilize security tools such as antivirus software, firewalls, and VPNs, and employ strong security practices. Regular software updates and data backups are crucial for protection against evolving cyber threats. (Buxton, 2023) Protecting oneself from cyber threats involves several key practices. First, using strong, unique passwords and enabling two-factor authentication adds an extra layer of security to your accounts. Keeping software and operating systems up to date ensures you have the latest security patches and protections against vulnerabilities. Additionally, installing reputable antivirus and firewall programs can help detect and block malicious activities. It is also crucial to be cautious about clicking on links or downloading files from untrusted sources to avoid malware infections. When using public Wi-Fi networks, a Virtual Private Network (VPN) should be used to protect data from being intercepted by cybercriminals. Lastly, regularly backing up data can help mitigate the impact of data loss due to cyber-attacks, ensuring critical information is not lost. (Saluja, 2023) With sustained efforts, there is hope for continued improvement in India's cybersecurity landscape. (Saluja, 2023)

CONCLUSION

As nations step into the digital age, cyber threats, particularly cyber warfare, pose a significant risk to national security. With the increasing reliance on the internet, nations have become more susceptible to various forms of cyberattacks, impacting all dimensions of state functioning, including political, social, financial, and personal domains. These attacks, often targeted by hostile state and non-state actors, can disrupt critical services, compromise sensitive information, and destabilize economies.

As cyber warfare is no longer limited to traditional hacking attempts; therefore, it encompasses a wide range of malicious activities, including espionage, disinformation campaigns, ransomware attacks, and disruptions to critical infrastructure such as financial institutions, power grids, and healthcare systems. Given the interconnectivity of modern digital systems, a single breach can have a domino effect, impacting not only national security but also the social and economic well-being of the citizens.

India, like many other nations, has recognized the urgency of addressing cyber threats and has adopted several measures to strengthen its cybersecurity framework. Initiatives such as the National Cyber Security Policy, the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC), and collaborations with international cyber defence agencies shows India's commitment to enhancing cyber resilience. Although India has implemented measures to counter these threats, it must ensure these strategies are fully executed and effectively enforced. Therefore, Developing and rigorously implementing a comprehensive and robust cybersecurity strategy is crucial for safeguarding against the growing menace of cyber warfare. This requires continuous investment in cyber defence capabilities, advanced threat intelligence mechanisms, and a highly skilled cybersecurity workforce. Additionally, fostering greater public-private partnerships and promoting cybersecurity awareness among businesses and individuals is essential to building a resilient cyber ecosystem. Moreover, international cooperation plays a crucial role in combating cyber warfare. Cyber threats transcend national borders, making it imperative for India to engage in global collaborations for intelligence sharing, joint cyber exercises, and policy development. Strengthening diplomatic efforts to establish norms for responsible state behaviour in cyberspace will further contribute to a secure digital landscape. As cyber warfare is subject to its dynamic nature, India must not only strengthen its digital infrastructure but also come up with a proactive approach to cyber defence. A robust and comprehensive cybersecurity strategy can be an answer to this problem.

REFERENCES

Bhattacharya, S., Ray, J., Sinha, S., & Sachdev, V. K. (2021). Cyber Warfare an Emerging Weapon of the 21st Century and the Biggest Non Violence Threat to a Nation. 10(11).

Buxton, O. (2023, July 14). Retrieved July 2024, from avast.com: https://www.avast.com/c-cyber-warfare

Buzan, B., Waever, O., & Wilde, J. D. (1998). In O. W. Barry Buzan, Security: A New Framework for Analysis. London: Lynne Rienner.

Buzan, B., & Hansen, L. (2009). The evolution of international security studies. Cambridge University Press.

Chadha, S. (2024, August 6). Cyber frauds cost India Rs 177 crore in FY24: How to protect yourself. Retrieved from business-standard.com: https://www.business-standard.com/finance/personal-finance/cyber-frauds-cost-india-rs-177-crore-in-fy24-how-to-protect-yourself-124080600123_1.html

Elbert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review, 19(4), 376-413.

Fortinet. (n.d.). History of Cyber Warfare and the Top 5 Most Notorious Attacks. Retrieved from fortinet.com: https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare

Gillis, A. S. (2023, March). cyberwarfare. Retrieved July 2024, from techtarget.com: https://www.techtarget.com/searchsecurity/definition/cyberwarfare

Hooda, L. S. (2021, March 15). DPG POLICY BRIEF Crafting India's Response to State-sponsored Cyberattacks. Retrieved from delhipolicygroup.org:

https://www.delhipolicygroup.org/publication/policy-briefs/crafting-indias-response-to-state-sponsored-cyberattacks.html

Kumar, R., & Mukherjee, N. (2013). Cyber Security in India: A Skill-Development Perspective.

Lok Sabha Secretariat. (2017, July). CYBER WARFARE AND NATIONAL SECURITY CHALLENG. Retrieved July 2024, from https://loksabhadocs.nic.in/: https://loksabhadocs.nic.in/Refinput/New_REFERENCES_Notes/English/Cyber_Warfare_and_National_Security_Challenges.pdf

Meity. (2023). Digital Personal Data Protection Act 2023.

Miller, C. M., & Kirda, E. (2020, October 12). The growing threat of cyberwarfare. Retrieved July 2024, from hindustantimes.com: https://www.hindustantimes.com/analysis/the-growing-threat-of-cyberwarfare/story-iiGha9WpqIKkQmPDdOLEHO.html

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers & security, 49, 70-94.

Saluja, B. (2023, March 5). CYBERSECURITY IN INDIA: TRENDS, THREATS, AND STRATEGIES FOR PROTECTION. Retrieved from community.nasscom.in: https://community.nasscom.in/communities/cyber-security-privacy/cybersecurity-india-trends-threats-and-strategies-protection

Sharma, M. (2013). India's Cyber Warfare Strategy In Next Decade. AIR POWER Journal, 8(3).

Standing Committee of Information and Technology. (2013-14). 52nd Report on Cyber Crime. New Delhi: MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY.

STANDING COMMITTEE ON FINANCE. (2022-2023). CYBER SECURITY AND RISING INCIDENCE OF CYBER/WHITE COLLAR CRIMES - 59th Report. NEW DELHI: LOK SABHA SECRETARIAT NEW DELHI.

Saraswat, A. (2024, December 31). Cyber Warfare in India: Analyzing Government's Approach to the 4th Dimension of War. Retrieved March 2025, from apacnewsnetwork.com: https://apacnewsnetwork.com/2024/12/cyber-warfare-in-india-analyzing-governments-approach-to-the-4th-dimension-of-war/#google_vignette

Sethi, N., & Thakur, A. (2017). CYBER WARFARE AND NATIONAL SECURITY CHALLENGES. NEW DELHI: LOK SABHA SECRETARIAT, NEW DELHI.

World Population Review. (2024). Internet Users by Country 2024. Retrieved from https://worldpopulationreview.com/: https://worldpopulationreview.com/country-rankings/internet-users-by-country