CENTRE FOR SECURITY STUDIES | ISSUE BRIEF

DECEMBER 2023

INDIA AND THE CYBER GOVERNANCE ARCHITECTURE

Bhavyl Bansal

Edited by: Aaryan Panchal

About the Author

Bhavyl Bansal is an undergraduate student candidate at the Jindal Global Law School and is a Research Intern with CSS at the Centre for Security Studies, JSIA.

About the Centre for Security Studies

The Centre for Security Studies (CSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof. Dr. Pankaj K. Jha. Researchers at CSS explore both regional and thematic topics in the broader field of international security studies to write issue briefs, policy briefs, defence white papers, and dialogue session reports on contemporary issues. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian, and religious conflict; civil wars and state failure; cyber and space warfare; resource-related security issues; the proliferation of weapons of mass destruction; defence economics and the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:


www.linkedin.com/company/jindal-centre-for-security-studies/


www.instagram.com/css_jsia/


https://twitter.com/Css_Jsia

Get in touch with us through email: css@jgu.edu.in

Important disclaimer

All views expressed in this publication belong to the author and do not reflect the opinions or positions of the Centre for Security Studies. While researchers and editors at CSS strive towards innovation, CSS as an organisation does not take any responsibility for any instance of plagiarism committed by the authors. The onus to ensure plagiarism-free work lies with the authors themselves.

IB2312010

Introduction

Cyber warfare has revolutionised and altered the way inter-state warfare has been and will be carried out in the 21st century. Although, there are numerous definitions of what constitutes 'cyberspace', one mutual denotation of these is the arcane nature of cyberspace that distinguishes it from other means of attacks.[1] Geographical demarcations don't exist and the anonymous feature of it further complicates the issues of jurisdiction and investigation.

Since the 1990s, a heavy and complete shift of dependence towards the digital space has been observed.[2] The magnitude of cyber-attacks can range from financial fraud to espionage and significant damage to the military and economic stability of a country. Thus, to protect themselves in the cyber arena, countries are required to invest strategically and heavily to secure themselves. Inevitably, it creates a divide between the monetary prowess of the developing and developed world. However, it is also true that the unprecedented operation of cyber warfare is such that even the most sophisticated and advanced technologies aren't spared by cyber ambushes. This issue brief shall explore the trajectory of cyber-attacks around the world, then focus on the Indian apparatus with emphasis on the existing framework and the vulnerabilities of the same.

[1] May, Larry. 2015. The Nature of War and Idea of Cyberwar. Cyber War: Law and Ethics for Virtual Conflicts. Oxford Academic.

[2] Mahmoud, Khalid Walid. 2013. Cyber Attacks: The Electronic Battlefield Arab Center for Research & Policy Studies.

Past Attacks

A meticulous cyber-attack is generally executed in tandem with electronic warfare, disinformation campaigns, anti-satellite attacks, and/or precision-guided munitions.[3] It requires unparalleled expertise, resources, and planning. The hacking of WikiLeaks, an Icelandic News Website, created havoc as numerous confidential documents of the US State Department about its missions around the world, were leaked on the website.[4] This event remains crucial in comprehending the impact of cyber-attacks and warfare in the modern world. Another shocking attack was the Stuxnet Worm of 2010, which infiltrated the computer systems and attacked Iran's nuclear facilities. It is estimated that the worm resulted in a 30% decrease in enrichment efficiency.[5] Allegedly, this worm was created by US and Israeli intelligence. The threat encompasses all spheres of the state, as observed in the 2016 US presidential elections, where interjection of Russian hackers was alleged.[6] The same surfaced in the 2020 elections as well, where few Russian businessmen openly admitted their involvement in tampering with the process of presidential elections.[7]

According to James Andrew Lewis of the Centre for Strategic and International Studies of Washington DC, Russian hackers are notorious for incessantly carrying out cyber espionage or

[3] Lewis, James Andrew. 2022. Cyber War and Ukraine. Centre for Strategic and International Studies.

[4] Mahmoud, Khalid Walid. 2013. Cyber Attacks: The Electronic Battlefield Arab Center for Research & Policy Studies.

[5] Alvarez, Joshua. 2015. Stuxnet: The World's First Cyber Weapon. Centre for International Security and Cooperation.

[6] Barnes, Julian. 2021. Russian Interference in 2020 Included Influencing Trump Associates, Report Says. The New York Times.

[7] Reuters.2022. Russia's Prigozhin admits Interfering in US Elections. Reuters.

attacks against their rivals. A paradigm indicates that cyber-attacks are proven to be more successful if they are carried out with other forms of attack. Prior to the 2014 invasion of Crimea, multiple DDoS attacks against Ukrainian forces by Russian media were carried out. Media, infrastructure, and confidential data served as important targets. Before commencing its 'military operations' in Ukraine last year, a broad cyber campaign was launched to target infrastructure and data.[8]

One of the most concerning features of cyber-attacks is that they can go undetected. For instance- the Snake malware which steals data, was detected in Ukraine in 2014 but it had been active seen 2011.[9] In 2019, the Indian authorities detected a malware attack at the Kundankulam nuclear plant, after six months such attack had been active.[10] The malware detected was similar to a Remote Access Trojan, which could have caused significant damage to the processes at the plant.

India and Cyber-Attacks

As India is making strides economically and politically, it is pertinent that such advances are accompanied by robust improvements in cyberspace as well. According to a study by Microsoft, India accounts for 13% of cyber-attacks in the Asia Pacific region.[11] Naturally, this incurs large

[8] Lewis, James Andrew. 2022. Cyber War and Ukraine. Centre for Strategic and International Studies.

[9] Baezner, Marie. 2018. Cyber and Information warfare in the Ukrainian Conflict. Centre for Security Studies, Zurich.

[10] Bhaskar, Utpal. 2019. India confirms malware attack at Kudankulam Nuclear Power Plant. Mint News.

[11] Kurmanath, K V. 2023. India emerges as top-3 target for nation-state driven cryber-attacks. The Hindu Business Line.

losses, a large-sized Indian enterprise loses an average of $10 million due to gaps in cyber security.[12]

An issue in India's cyber security model is its heavy dependence on technology manufactured by other states. India's vulnerability to cyber-attacks isn't a novel conundrum. For instance, Operation Shady Rat was a cyber espionage campaign by a group of hackers that were stealing confidential data from more than 70 government and private organisations across 14 countries, India being one of them.[13] The banking sector continues to remain at perpetual peril; post-demonetisation, as online transactions gained popularity, so did phishing scams and data scams.

As discussed earlier, cyber-attacks are used in aid, and compounded with other types of attacks to maximise the damage. This manifested in a catastrophe during the 26/11 Mumbai Attacks when police found that terrorists heavily relied on digital intelligence. A similar pattern was observed in the Pulwama Attacks 2019.[14]

In 2017, India fell victim to Firewall, a malware that was capable of downloading and running code on the targeted computer and spying on data. According to Check Point, a security firm, India was one of the worst affected countries by this malware.[15] The same firm stated that Firewall is a creation of Rafotech which is based in Beijing. India needs to adopt an extremely vigilant approach pertaining to its data, especially considering that India shares a sensitive relationship with its neighbours. In 2021, the Ministry of Electronics and Information Technology (hereafter referred

[12] Microsoft Stories. 2018. Cybersecurity threats can cost large organisations in India as an average of US$ 10.3 million in economic losses. Microsoft India.

[13] Alperovitch, Dmitri. 2011. Revealed: Operation Shady Rat. McAfee

[14] Gupta, Shishir. 2019. Speeches, cyber trail in India's Pulwama Proof establish role of Jaish. Hindustan Times.

[15] Tech Desk. Fireball: This Chinese Malware has infected 250mn PCs, India 'worst hit. The Indian Express.

to as MeitY), alerted users of 27 Indian banks that there persists a grave risk of intrusion by a new banking trojan malware.[16]

According to Resecurity, an American cybersecurity company, the information of over 80 crore individuals, including those affiliated with the Indian Council of Medical Research, was leaked on the dark web.[17] Investigations discovered that the entire Aadhaar dataset could be sold for $80,000. As the government remains enthusiastic for its vision to digitalise the nation and espouses citizens to actively link their Aadhar details with other aspects of their identity, such negligence pertaining to data privacy cannot be sustained in the long run.[18]

Furthermore, a report by Seqrite, an Indian security firm, highlights that Pakistan-based hackers have been trying to interject with the cyber security of the Indian Army and eminent educational institutions such as the IITs.[19] Additionally, as India hosted the G-20 summit this year, there were stronger allegations of Pakistani groups targeting government websites. Although, this back-and-forth cyber espionage and attacks have become common between India and Pakistan. Pakistani authorities incessantly remain suspicious and allege that Indian authorities deploy means of cyber

[16] Ghosh, Debangana.2021. Beware of Trojan malware attack, MeitY warns customers of 27 major banks. The Hindu Express Line.

[17] Resecurity. 2023. PII Belonging to Indian Citizens, including their Aadhar IDs, Offered for Sale on the Dark Web. Resecurity.

[18] Resecurity. 2023. PII Belonging to Indian Citizens, including their Aadhar IDs, Offered for Sale on the Dark Web. Resecurity.

[19] Saini, Neha. 2023. Pakistan based threat actors attacking IITs, Indian Army. Mint News.

espionage against top Pakistani officials.[20] This apprehension became grave when the Indian government was found to be using Pegasus, an Israeli Spyware.

Unequivocally, India needs to pace itself to combat the drawbacks of the cyber world, as it embarks to become more tech-savvy and a dominant global player. As mentioned earlier, an attack on India's nuclear plant went undetected. Additionally, attacks capable of tampering with data and carrying out surveillance have unfortunately become common, even against the highest officials and institutions of the state.

While the threat from other states and organisations with nefarious motives is ubiquitous, cyber threats from state institutions are another facet of the problem. In 2023, Apple Inc. warned a few oppositions political leaders and journalists, that their iPhones might be the target of state-sponsored surveillance. This is clearly an encroachment on democratic values and privacy of individuals, that cannot be overlooked. While the veracity of this claim is still unclear, any encroachment on democratic values and the privacy of individuals cannot be overlooked.[21]

India's Institutional and Legislative Framework to Combat Cyber-Attacks

In the state itself, there are various stakeholders having a cogent cyber governance framework, such as MeitY, the Ministry of Defence, the Ministry of Home Affairs, and the Intelligence agencies.[22] The National Cyber Coordination Centre is a surveillance agency under the jurisdiction of the Ministry of Home Affairs. Additionally, the Indian Computer Emergency Response Team (CERT-IN) is another pivotal nodal agency established in 2004 under MeitY, that deals with cyber security threats.[23] Last year, CERT-IN released directives with respect to proper procedures for

[21] Al Jazeera. 2023. 'State-sponsered' attacks on phone of India opposition leaders. Al Jazeera.

[22] Lt Gen Panwar, R S. 2020. Cyberspace Governance In India. Future Wars.

[23] PIB Delhi. 2018. Cyber Security. Ministry of Home Affairs.

reporting cyber incidents. Under the Ministry of Home Affairs, the Indian Cyber Crime Coordination Centre (I4C) is operative, to mitigate the threats of cyber terrorism and attacks.[24] Whereas, under the Ministry of Defence, a defence cyber agency is designated to focus on countering cyber-attacks against the army, navy, and air force.

The National Critical Information Infrastructure Protection Centre (hereafter referred to as NCIIPC) was established in 2014 under the IT Act 2000[25]. The IT Act amendment defined Critical Information Infrastructure as 'those facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation'.[26] The NCIIPC is designated as the National Nodal Agency to safeguard critical information infrastructure.[27] Its duties include protecting the vulnerabilities of the cyberspace from threats of cyber warfare, providing leadership to the government with respect to identifying and circumventing the threat, undertaking research and development tasks with respect to cyber security, and producing novel and effective strategies for implementation of protection policies, etc.[28]

The critical sectors that come under the purview of NCIIPC are power and energy, banking and financial institutions, information and communication technology, transportation, and e-governance and Strategic Public Enterprises.[29] Safeguarding CII requires the trust and collaboration of various institutions. This poses an impediment for NCIIPC, and it has been conscious of it. The NCIIPC follows a vulnerability/threat/risk analysis for comprehending the vulnerability of each sector; the NCIIPC shall benefit from having sector-specific guidelines and

[24] Ministry of Home Affairs, I4C.

[25] The Information Technology Act 2000.

[26] Section 70A, Information Technology Act 2000.

[27] NCIIPC.gov.in

[28] Ibid (19)

[29] Datta, Saikat. 2016. The NCIIPC and its evolving Framework. ORF.

adopt a holistic approach that is cognisant of the inter-dependency of different sectors, rather than focusing on limited critical sectors.[30]

When it comes to the legislative framework of India, recently India passed the **Digital Personal Data Protection** (hereafter referred to as the DPDP) **Act 2023**.[31] This was a pertinent step in India's cyber governance architecture regarding safeguarding privacy, and this act was long overdue as it had been in talks for more than half a decade. The DPDP Act has reduced obligations for businesses with respect to security and transparency requirements, that were earlier proposed in the bill. The DPDP act simplifies the regulator structure but a critique of the same can be that the central government has been vested with vast and unguided powers.[32] Additionally, DPDP focuses on significant data fiduciary (SDF), and the act also directs the appointment of a data auditor, and data protection officer, and conducts a data protection impact assessment.[33]

However, in the realm of protecting the cyber security of the state as well, the laws are primarily governed by the IT ACT 2000. Section 66F of the mentioned act pertains to provisions relating to cyber terrorism against the sovereignty of the state.[34] Additionally, the National Cyber Security Policy was introduced in 2013 to provide a comprehensive framework for strengthening cyber security at a national level.[35] The Indian Penal Code 1860, and the Unlawful Activities (Prevention) Act 1967, contain additional provisions pertaining to cyber terrorism as well.

[30] Datta, Saikat. 2016. The NCIIPC and its evolving Framework. ORF.

[31] Digital Personal Data Protection Act 2023.

[32] Burman, Anirudh. 2023. New Data Protection Law. Carnegie India.

[33] Kalra, Lalit. 2023. Decoding the Digital Personal Data Protection Act 2023. EY.

[34] Section 66F, The Information Technology Act 2000.

[35] National Cyber Security Policy 2013.

Conclusion

While India does have a legislative framework that covers aspects of cybercrime, and specialised bodies designated to strengthen India's cyber security against unwanted interference; considering the dynamic nature of the cyber world, they do not look adequate. India needs to make astute efforts to keep up with the pace of cyber offenders to develop a robust cyber governance architecture.

Despite the existence of these agencies, India has incessantly witnessed intrusions in cyberspace and remains extremely vulnerable. In the Union Budget 2023, MeitY had been allocated INR 625 crores to improve the cyber security mechanisms.[36] Out of this amount INR 400 crores has been reserved for cyber security projects and the rest is for the operations of CERT-IN.[37] This is an imperative step as it is an undisputed fact that technology is the future, and its influence has infiltrated and redrawn the traditional borders and strategies for attacking the state.

Hence, it is crucial for India to be cognizant and not underestimate the cyber damages that can undermine its domestic and international standing. Other countries are also actively seeking to enhance their cyber security measures. Cyber security holds a paramount position in defence and conflict strategies. For instance- the US for a long time has been constantly trying to upgrade its cyber prowess, to protect itself from Chinese and Russian hackers, and other intruders. India should take advantage of its improved diplomatic relationships to seek out better collaborative opportunities with respect to upgrading cyber security models. However, India should be cautious with this collaboration turning into dependence which is a paramount drawback that shall hinder our progress.

On the surface, it might be perceived that India's governance structures are sufficient; while it is true that Indian authorities are determined and committed towards betterment. For instance- the recently organised mock drills 'Bharat National Cyber Security Exercise' in October 2023 to check

[36] Press Information Bureau. Government of India.

[37] Yadav, Pihu. 2023. Budget 2023, government to spend Rs. 225 crores on Cybersecurity Response Team. CNBC.

the preparedness of the state, we witnessed the Aadhar leak on the dark web shortly after. Therefore, this should be taken as an indication of the lacuna that needs to be filled with the aid of better resources, intelligence, policy framework and regulations, and autonomy to the enforcement units.