CENJOWS

WEB ARTICLE
WA/17/24

INDIAN CYBERSPACE: THREAT PREVENTION

MS SHREYA MAMGAIN

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

INDIAN CYBERSPACE:

THREAT PREVENTION

Ms Shreya Mamgain is an alumna of Lady Sri Ram College for Women and Hindu College of University of Delhi where she pursued B.A. (HONS) History and M.A. History respectively. She is currently pursuing Ph.d. from the Department of East Asian Studies, University of Delhi.

Introduction

According to the Department of Defence (DOD)[1], cyberspace is defined as a global domain within the information environment (IE) consisting of the interdependent networks of information technology infrastructure and resident data, including the internet, telecommunications networks, computer systems and embedded processors and controllers[2].

In recent times, cyberspace has become a new domain of warfare. However, this does not mean that traditional warfare is being replaced by these new means of conflict. Across the world, there have been several cyberspace attacks that have not only led to data breaches and concerns for invasion of privacy but also affected the daily administrative as well as infrastructural tasks. Some of the examples of such attacks include the cyberattacks between Ukraine and Russia and the cyberattacks on JAXA[3], which is currently under investigation[4]. These attacks have increased in recent times and have become one of the biggest concerns of governments around the world.

Countries have adopted different policies in order to tackle these newly emerging threats. For example, in Japan the Public Security Intelligence Agency (PSIA) has been tasked with ensuring the protection of the public[5]. Similarly, in India the Computer Emergency Response Team- India (CERT-In) has been tasked with functions analogous to the PSIA. A major development in India that signals the government's as well as the armed forces commitment to protect cyberspace from further attacks is the release of the Joint Doctrine for Cyberspace Operation by the Chief of Defence Staff (CDS) General Anil Chauhan during the Chiefs of Staff Committee (COSC) in New Delhi[6] in June 2024. This doctrine is essential as it will provide the Indian Armed Forces guidance to conduct cyberspace operations in the complex military operating in today's environment. This article aims to analyse the attempts of the government agencies including our armed forces to prevent attacks on the Indian Cyberspace by various state and non-state actors.

What is Cyberspace?

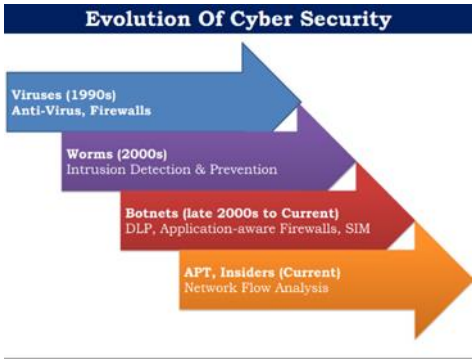
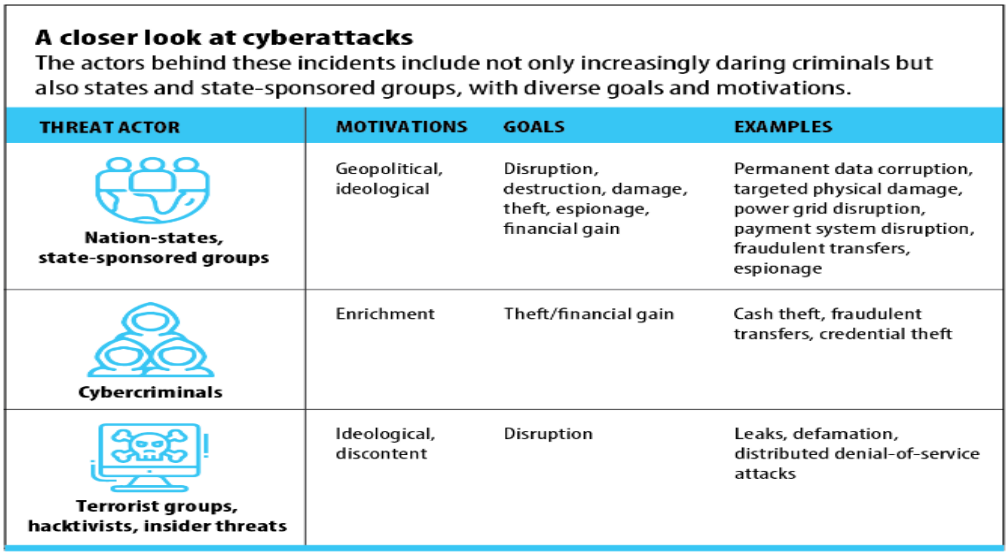


FIG 1 & 2: The above diagrams show the evolution of Cyber Attacks and Cyber Security across the world during various time periods. (Images taken from- https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf)

Cyberspace according to the 2013 National Cyberspace Security Policy of India, is a complex environment that consists of interactions between people, software and services that is supported by a worldwide distribution of Information and Communication Technology (ICT) devices and networks[7]. Due to its intricate, complex and highly fragile nature, the cyberspace is prone to attacks by various malicious entities that are either affiliated to a state or are non-state actors.

The figure given below shows us the different entities that assault cyberspace.



A closer look at cyberattacks

The actors behind these incidents include not only increasingly daring criminals but also states and state-sponsored groups, with diverse goals and motivations.

THREAT ACTOR	MOTIVATIONS	GOALS	EXAMPLES
Nation-states, state-sponsored groups	Geopolitical, ideological	Disruption, destruction, damage, theft, espionage, financial gain	Permanent data corruption, targeted physical damage, power grid disruption, payment system disruption, fraudulent transfers, espionage
Cybercriminals	Enrichment	Theft/financial gain	Cash theft, fraudulent transfers, credential theft
Terrorist groups, hacktivists, insider threats	Ideological, discontent	Disruption	Leaks, defamation, distributed denial-of-service attacks

Source: European Systemic Risk Board. 2020. "Systemic Cyber Risk." https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

FIG 3: This figure depicts the various entities that attack the cyberspace. (Image taken from- https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm).

In order to counter and repel any attacks by these entities, the Indian Government formulated various initiatives such as Cyber Surakshit Bharat, National Cybersecurity Coordination Centre (NCCC), Cyber Swachhta Kendra and Information Security Education and Awareness Project (ISEA). However, despite these efforts the number of cyberattacks have increased and evolved.

According to a report by Check Point Technologies Ltd., an organisation in India faced an average of 2,807 attacks in the first quarter of 2024, a 33% yearly increase, making it the most targeted country worldwide. It also revealed that the most heavily targeted sectors were education & research, government & military and healthcare. However, the hardware vendor industry saw a substantial increase in cyberattacks[8].

The evolution of the cyberattacks and methods of cybersecurity from Viruses (Anti-Virus and Firewall) to APT[9] and Insiders (Network Flow Analysis)[10] shows us the importance of updating our knowledge and methods to protect our cyberspace that is increasingly being threatened.

Threats To The Indian Cyberspace

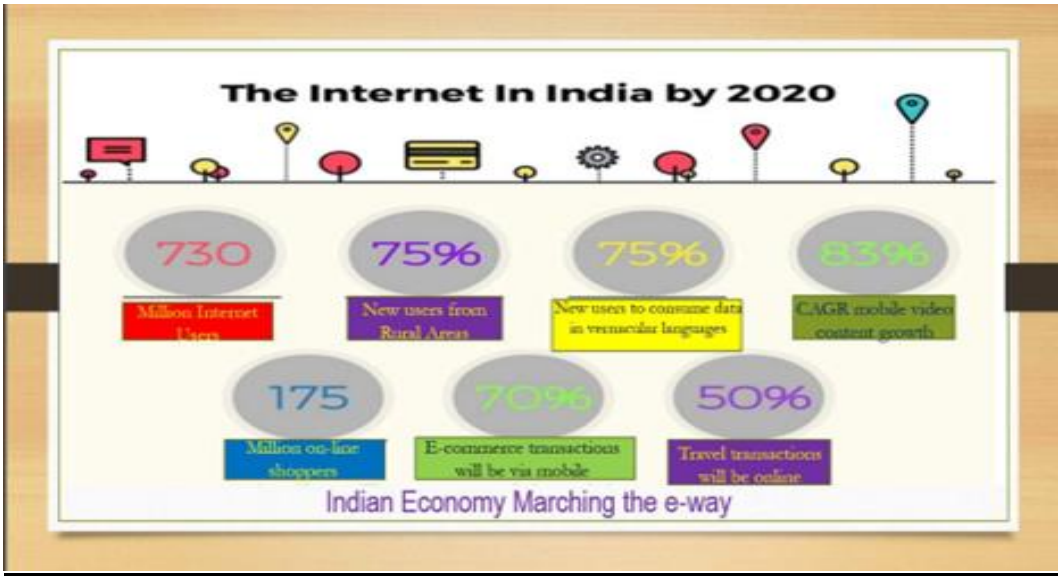


Fig 4: This image depicts the interdependence of the Indian Economy on Cyber Space. (Images taken from- https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf)

In recent years, the technological dependence of warfare has increased. The domains of space and cyber have become the new arenas of conflicts. As a result, the Global as well as the Indian Cyberspace as seen attacks by malicious entities. Some of the most recent of these attacks include- the attack on the software company CDK Global where in the hackers demanded a tens of milliions of dollars in ransom[11] and the hacking of the X(Formerly Twitter) Handle of Canara Bank[12].

Recently, a report by Symantec Threat Hunter Team, a part of Broadcom disclosed that Cyber Espionage groups associated with China have been linked with a long-running that has infiltrated several telecom operators located in a single Asian country since 2021[13]. Similarly, the malware campaign that is linked to Pakistan called "Operation Celestial Force" that is currently still in operation and is increasingly utilising an expanding and evolving malware suite- indicating that operation has likely seen a high degree of success targeting users in the Indian Subcontinent[14] has been reported.

According to the India Cyber Threat Report 2023 by Data Security Council of India (DSCI)[15] has predicted that in 2024 some of the major cyberspace threats would include- Ransomware and Digital Extortion, MFA Fatigue Attacks[16], Event Based Attacks, Phishing/Vishing attacks & Dating App Scams, Exploitation of Supply Chains, AI Powered Malware and use of Deep Fake for Deceptive Social Engineering[17]. The report has highlighted some of the ways[18] in which these threats can be mitigated and prevented:

1. **Vigilance against APTs**- It is imperative to maintain a heightened state of alertness and preparedness to face APTs that utilise multi-vector attacks, zero-day vulnerabilities and sophisticated malware. Prioritising the establishment of comprehensive monitoring and incident response capabilities to swiftly detect and contain these threats, mitigating any potential damage to systems and data.
2. **Robust Ransomware Defense Strategy**- Creation and implementation of a defense system that has been specifically tailored to combat ransomware. This type of a defense system should encompass regular backups of critical data, network segmentation, rapid detection and isolation of affected systems. A crucial component is the development of a well-prepared and tested incident response plan to effectively mitigate the impact of potential ransomware attacks.
3. **Integration of Emerging Technologies**- Embracing the transformative potential of emerging technologies and innovations. It is imperative to proactively leverage the opportunities and benefits of these technologies with caution and awareness being exercised.
4. **Collaboration and Coordination**- By creating a collaborative ecosystem, one can stay one step ahead of evolving threats.

Cyberattacks also are a major threat to our financial institutions. In a statement given by Christine Lagarde in February 2020, warned that a serious financial crisis can be triggered by a cyberattack[19]. Thus, the changing nature and the growth of these threats by vicious entities, we find ourselves in a precarious situation.

This is exasserbated by the fact that in the recent times Indian Economy has become increasingly dependent on Cyber space. Known as the “fifth domain of warfare” along side space ehich is the “fourth domain of warfare”[20], cyber is becoming an increasingly important area of interest for most states across the world.

Cyberspace Protection: Prevention and Protection

In order to protect the Cyber space from any vicious entities that may cause harm, in 2013 the Indian Governement drafted the National Cyberspace Security Policy of India. The policy stated that it's vision is to "build a secure and resilient cyber space for citizens, businesses and government"[21]. The policy has highlighted several strategies that it would implement in order to achieve its vision.

However, the creation of a policy is not enough. There are several measures that can be undertaken not just at the individual but also at the level of corporations and governments. Some of these steps[22] include-

1. **Secure Networks and Databases-** Protection of networks by setting up firewalls and encrypting information. This ensures that the risk of cyber criminals gaining access to confidential information is minimized.
2. **Education of Employees-** Awareness amongst employees regarding security and protection of information.For instance, employees should be trained to recognise fake anti-virus warning messages and alert IT as soon as they notice anything questionable occuring.
3. **Creation of Security Policies and Practices-** Establishment of practices and policies to protect from cyber attacks as well as to provide guidelines for resolving issues if they arise.

The government has also instituted bodies such as CERT-In and implemented policies for bringing awareness to the masses such as Information Security Education and Awareness Project (ISEA). But these efforts should be for overall protection and not just the protection of a few groups. Due to the importance of the fourth and fifth domains of warfare, collaboration and co-operation becomes a key for threat mitigation and prevention. For instance, Lt. Gen. Pannu in his essay points out that "space infrastructure requires a cybershield"[23]. Such collaboration does not just stop here. Collaboration between the primary domains i.e. land, water and air is also necessary. Inter-governmental agencies partnership also crucial. Such partnerships would allow agencies like JAXA and ISRO to look at the different methodologies that are in use amongst hackers and create viable technologies that will prevent these attacks. Greater co-operation and collaboration therefore, may help us tackle future threats or eliminate the threats present currently.

Conclusion

The Joint Doctrine for Cyberspace Operation is a great step for cooperation between the tri-services. It also serves to provide a blueprint to our armed forces in times of a cyberware. However, the time of cyberware has already begun and while the doctrine is a great move, it is not enough. More technologies and great cooperation and collaboration is needed not just amongst the tri-services, but also amongst intergovernmental agencies. Education, awareness and creation of a system of "cybershield" are important to achieved to protect the Indian Cyber Space from being targeted.

DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Endnotes

[1] The US Department of Defense (DOD), is an executive branch department of the federal government of United States that is charged with coordinating and supervising all agencies that work towards security of the nation.
[2] Congressional Research Service; In Focus, Defense Primer: Cyberspace Observations, 14 December 2023. Accessed on 20 June 2024. https://sgp.fas.org/crs/natsec/IF10537.pdf.
[3] Also called the Japan Aerospace Exploration Agency.
[4] Japan's cyber space agency hit by repeated cyberattacks since last year. Accessed on 24 June 2024. https://www.japantimes.co.jp/news/2024/06/21/japan/jaxa-cyberattacks/.
[5] Overview of Threats in Cyberspace, 2023. Accessed on 20 June 2024. https://www.moj.go.jp/content/001398997.pdf.
[6] CDS Gen Anil Chauhan releases Joint Doctrine for Cyberspace Operations. Accessed on 20 June 2024. https://pib.gov.in/PressReleasePage.aspx?PRID=2026240 .
[7] National Cyber Security Policy-2013. Accessed on 20 June 2024. https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.
[8] Cyber Attacks surge globally in Q1 2024, India among the most targeted nations: Report, 12 May 2024. Accessed on 21 June 2024. https://timesofindia.indiatimes.com/technology/tech-news/cyber-attacks-surge-globally-in-q1-2024-india-among-most-targeted-nations-report/articleshow/110041081.cms.
[9] APT is also known as Advanced Persistent Threat that is used by organised hackers to steal private data.
[10] Dr. VK Saraswat, Cyber Security. Accessed on 21 June 2024. https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf.
[11] Anthony Robledo, Bailey Schulz and Betty Lin Fisher, Auto dealer system updates to take 'several days' following CDK hack, ransom demand, USA Today. Accessed on 24 June 2024. https://www.usatoday.com/story/money/cars/2024/06/21/cdk-cyberattack-ransom-demands-report/74175607007/.
[12] Canara Bank Says X Handle "Compromised", Hacker changes username. Accessed on 24 June 2024. https://www.ndtv.com/india-news/canara-bank-says-x-handle-compromised-hacker-changes-username-5952073.
[13] Chinese Cyber Espionage Targets Telecom Operators in Asia since 2021. Accessed on 24 June 2024. https://thehackernews.com/2024/06/chinese-cyber-espionage-targets-telecom.html.

[14] Pakistan-Linked Malware Campaign Evolves to Target Windows, Android, and macOS. Accessed on 24 June 2024. https://thehackernews.com/2024/06/pakistan-linked-malware-campaign.html.
[15] It is a non-profit industry body that was set up by nasscom.
[16] Multi-Factor Authentication (MFA) Fatigue Attacks are also known as MFA Bombing or MFA Spamming. In such type of attacks, the malicious entity repeated pushes second factor authentication requests to the victim to confirm their identity. This is a form of a social engineering attack.
[17] DSCI, India Cyber Threat Report 2023, pp.67.
[18] DSCI, India Cyber Threat Report 2023, pp.73.
[19] Maurer Tim and Nelson Arthur, Cyber Threats to the financial system are growing, and the global community must cooperate to protect it. Accessed on 28 June 2024. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.
[20] Lt. Gen. PJS Pannu, Why India's space and cyber domains need well-built 'cyber shield'. Accessed on 28 June 2024. https://www.firstpost.com/opinion/why-indias-space-and-cyber-domains-need-well-built-cybershield-13770264.html.
[21] National Cyber Security Policy-2013. Accessed on 24 June 2024. https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
[22] Protect your company from Cyber Attacks. Accessed on 27 June 2024. https://www.mass.gov/info-details/protect-your-company-from-cyber-attacks.
[23]Lt. Gen. PJS Pannu, Why India's space and cyber domains need well-built 'cyber shield'. Accessed on 28 June 2024. https://www.firstpost.com/opinion/why-indias-space-and-cyber-domains-need-well-built-cybershield-13770264.html.