CBW Magazine
Journal on Chemical and Biological Weapons
Summer / January-June 2023
ISSN: 0974-0619

MANOHAR PARRIKAR idsa
MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

Navigating the Cyber-Biosecurity Landscape: A National Security Imperative for India

Animesh Roul

Mr Animesh Roul is the Executive Director of the Society for the Study of Peace and Conflict, New Delhi.

Summary

The shifting terrain of national security threats has broadened to include not just traditional geopolitical and military risks, but also challenges emerging from the realms of cyber and biology, forming what is termed as cyber-biosecurity. This novel idea of cyber-biosecurity arises as a blend, combining the swiftly merging fields of cybersecurity and biosecurity. While each area has previously had its distinct focus and specialized knowledge, the changing landscape shows that they are progressively intertwining in intricate and impactful ways.

The ever-evolving landscape of national security threats has expanded to encompass traditional geopolitical and military risks and challenges arising from the cyber and biological domains termed cyber-biosecurity. This hybrid concept of cyber-biosecurity emerges as an innovative fusion, encapsulating the rapidly converging disciplines of cybersecurity and biosecurity. While each domain has historically commanded its attention and expertise, the evolving landscape reveals they are increasingly intersecting in complex and consequential ways.[1] Such a confluence produces new challenges that can remotely disrupt biomedical and bio-industrial processes, compromise digital health records and medical devices, and even jeopardize high-containment laboratories (e.g., BSL-3 or BSL-4). This amalgamation extends the horizon of vulnerabilities, manifesting multifaceted risks that traverse critical sectors, including manufacturing, emergency medical systems, public health, healthcare, the biochemical industry, food production, agriculture and eventually, national security. Undoubtedly, the COVID-19 pandemic has helped raise awareness about biosecurity and public health to a reasonable extent in India and the region. **This commentary aims to provide an overview of the cyber-biosecurity landscape, identifying the challenges and opportunities it presents for India's biomedical Institutions, including hospitals, laboratories and pharma companies. It also underscores India's vulnerabilities and strategic imperatives in this new frontier of security.**

The integration of cybersecurity and biosecurity is a critical issue that is coming to the forefront, especially as healthcare

infrastructures, among other critical life science and biotechnological sectors, become susceptible to cyber threats. Within the Indian context, this vulnerability manifested in the escalating number of cyber-attacks on healthcare institutions and pharma laboratories. Data collated by cybersecurity agencies in India indicates that from January to November 2022 alone, approximately 1.9 million cyber-attacks targeted India's healthcare systems, making hospitals easy targets for cybercriminals.[2] The suspected ransomware attacks on the country's premier hospitals, such as All India Institute for Medical Science (AIIMS), have become a regular affair, primarily disrupting the online services and theft of patient data. In November 2022 and June 2023, ransomware attacks were detected at two major hospitals, AIIMS and Safdarjung Hospital in New Delhi.[3] Although they successfully recovered their compromised databases, challenges and vulnerabilities remain, especially in its digital services. In June 2023, a major leak of CoWIN data via the Telegram app was reported. This data leak exposed several personal and health details, including names, Aadhaar IDs, mobile numbers, voter IDs, passports and COVID vaccination status of high-profile individuals, including politicians, industrialists and business people.[4]

In late November 2022, over 6,000 attempts were made by a Hong Kong based entity to hack the server of the Indian Council of Medical Research (ICMR), the apex body in India for biomedical research. Fortunately, the ICMR server remained secure due to enhanced security measures and a robust updated firewall.[5] Ransomware attacks were reported on the burgeoning Pharma companies in India, too. In late March this year, one of India's largest drug manufacturers, Sun Pharma's operations, was affected due to a ransomware attack. The attack breached file systems and stole company as well as personal data.[6] Similar ransomware attacks were reported from Ipca Laboratories and Aarti Drugs Ltd in September 2022. Both suffered data theft and extortion from the BianLian ransomware group, which demanded a huge amount of money for the decryption key, and it put up part of the stolen data for sale on the dark web.[7]

Indeed, biomedical institutions, especially the top hospitals (like AIIMS) where political and business elites have their health records, have become lucrative targets for state-sponsored or non-state cybercriminals. The increased digitization of medical records and reliance on online systems has amplified the risks multifold. Previously, in India, several notable cyber incidents have impacted the healthcare sector, emphasizing hospitals, laboratories, and related institutions. One of the major ones was the WannaCry Ransomware Attack in 2017. This was part of a worldwide cyberattack which affected institutions across India, including healthcare entities, power grids and banks.[8] The malware had encrypted files and demanded a ransom in Bitcoin for decryption. It reportedly caused major disruption of patient care services, financial loss, and potential compromise of patient information. Though the attack was not focused towards health and biotech industries, the footprint was spread across sectors, especially digitized (internet and computers) organizations.

The above events suggest that cyberattacks exacerbated vulnerabilities and compromised millions of sensitive medical and personal data, causing substantial financial losses and unprecedented disruption in healthcare services. Arguably, the vulnerability of the biomedical sector to cyber threats in India highlights the need

for stronger cybersecurity measures, comprehensive regulations, and robust incident response mechanisms. Continued investment in security infrastructure, security audits in regular intervals, multi-factor authentication, employee training, and collaboration with cybersecurity experts are vital to protecting the health data and critical services provided by the healthcare and life science sectors. The AIIMS incidents indicate a pattern of risks common to healthcare institutions worldwide. They reflect the growing importance of cybersecurity in healthcare, where patient data, research, and day-to-day operations are increasingly digital and interconnected.

Countries like the United States, Israel and a few European countries have already started or are in the process of integrating cyber-biosecurity into their national security strategies. The rise of state-sponsored cyber-attacks and the proliferation of biotechnologies necessitate a unified approach to these challenges. Despite the stepped-up measures, ransomware attacks in the US disrupt healthcare services regularly.[9]

This vulnerability is particularly concerning in light of India's ambitious drive to digitize healthcare, which is now being impeded by recurrent cyberattacks. Cybersecurity experts have sounded the alarm over the insufficient resilience of healthcare cybersecurity systems and the absence of stringent data protection legislation. While cybersecurity has primarily fallen on individual healthcare institutions, there is a growing argument that safeguarding such a vast corpus of sensitive data should be a government or national responsibility.

Emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and advanced biotechnologies create new opportunities and vulnerabilities. These technologies can be weaponized to create sophisticated threats that exploit vulnerabilities in both digital and biological spheres.

In this intricate landscape of technology and security, manoeuvring cyber-biosecurity challenges becomes a non-negotiable national imperative for India. The country is not merely a rising technological powerhouse but also a state entangled with various biosecurity complexities. Addressing these challenges necessitates a multi-layered approach that includes robust cybersecurity frameworks, regular security assessments, specialized staff training, and deploying cutting-edge security technologies. As the sectors of public health, manufacturing, emergency medical services, and national defense, among others, come under the widening ambit of cyber-biosecurity threats, the call for a fortified security posture is not just timely; it is critical for both the healthcare organizations and the nation at large. India has established agencies like the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC) for cybersecurity. The ransomware attack on the AIIMS recently prompted the government to formulate a national cybersecurity response framework (NCRF).[10]

Conclusion

The overall biosecurity framework remains fragmented and less prioritized in India. This underscores the immediate necessity for healthcare organizations to bolster their cybersecurity defenses. Nonetheless, a centralized, government-led approach to enhance the nation's cyber-biosecurity infrastructure across critical sectors is indispensable for India's long-term resilience and technological ambitions. The country's goals of becoming a global leader in

technology and healthcare hinge on its capability to safeguard cyber and biological assets. Therefore, cyber-biosecurity should not merely be viewed as a health or economic issue but as a priority for national security.

Endnotes:

[1] For better understanding of this emerging hybrid concept, See, for example, Dov Greenbaum (ed), *Cyberbiosecurity: A New Field to Deal with Emerging Threats*, Springer, 2023. Also, Jean Peccoud, Jenna E. Gallegos, Randall Murch, Wallace G. Buchholz, Sanjay Raman, "Cyberbiosecurity: From Naive Trust to Risk Awareness", *Trends in Biotechnology*, Vol. 36 (1), 2018, pp. 4-7, https://www.sciencedirect.com/science/article/pii/S0167779917302767

[2] "Indian healthcare system needs robust cybersecurity infra. Here's what experts say", *Livemint,* April 23, 2023 https://www.livemint.com/news/india/india-healthcare-system-robust-cybersecurity-infrastructure-aiims-cyberattack-safdarjung-hospital-sun-pharma-cyberattack-11682223039473.html

[3] "Malware attack detected at AIIMS; cyber security systems neutralise threat", *Economic Times*, June 06, 2023, https://economictimes.indiatimes.com/tech/technology/malware-attack-detected-at-aiims-cyber-security-systems-neutralise-threat/articleshow/100800906.cms

[4] "CoWIN data breach | Cybersecurity watchdog to probe claims that user information leaked on Telegram", *CNBC TV18*, June 12, 2023, https://www.cnbctv18.com/technology/has-your-covid-19-vaccination-data-leaked-on-telegram-16909031.htm

[5] "Nearly 6,000 attempts to hack ICMR server thwarted on 30 Nov, website safe", *Livemint*, December 06, 2022 https://www.livemint.com/news/india/nearly-6-000-attempts-to-hack-icmr-server-thwarted-on-30-nov-website-safe-11670342847017.html#

[6] "Sun Pharma says revenue may decline as operations hit due to ransomware attack", *Indian Express*, March 27, 2023, https://indianexpress.com/article/business/companies/sun-pharma-revenue-operations-ransomware-attack-8520897/

[7] https://ciso.economictimes.indiatimes.com/tag/ipca+laboratories

[8] "WannaCry did hit India and even central govt portal. So why did Centre downplay the ransomware attack?", *India Today*, June 19, 2017, https://www.indiatoday.in/mail-today/story/ransomware-wannacry-cyberattack-global-ransomware-attack-india-983427-2017-06-19

[9] "Ransomware attack disrupts healthcare services in at least three US states, *Economic Times*, August 06, 2023, https://economictimes.indiatimes.com/tech/technology/ransomware-attack-disrupts-healthcare-services-in-at-least-three-us-states/articleshow/102465001.cms

[10] "AIIMS ransomware attack led to new SOP on cyber breaches: Ex-cybersecurity chief Pant," *Hindustan Times*, July 02, 2023, https://www.hindustantimes.com/india-news/aiims-ransomware-attack-led-to-new-sop-on-cyber-breaches-ex-cybersecurity-chief-pant-101688321198625.html