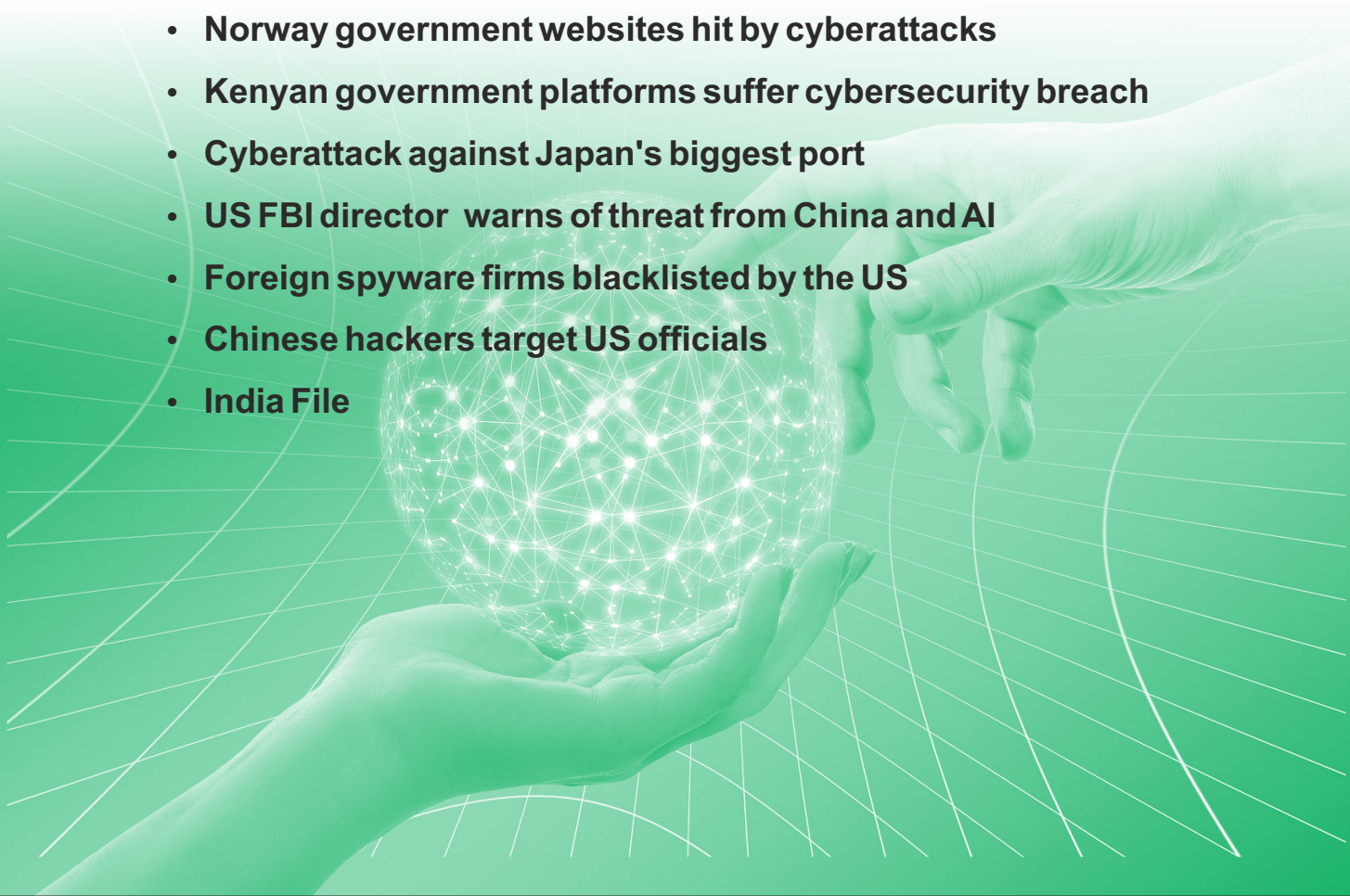
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

August 2023

- Takeaways from Prime Minister Narendra Modi's Visit to France
- Data leak from Bangladesh's government website
- New EU-US data transfer pact
- Norway government websites hit by cyberattacks
- Kenyan government platforms suffer cybersecurity breach
- Cyberattack against Japan's biggest port
- US FBI director warns of threat from China and AI
- Foreign spyware firms blacklisted by the US
- Chinese hackers target US officials
- India File



Takeaways from Prime Minister Narendra Modi's Visit to France

Prime Minister Narendra Modi paid an official visit to France and the United Arab Emirates (UAE) from 13-15 July 2023. While this year marks the 25th anniversary of the India-France strategic partnership, the visit to the UAE provided an opportunity to take forward the India-UAE Comprehensive Strategic Partnership. The visit to Paris highlighted the importance of technological cooperation to promote research partnerships and technologies that ensure self-reliance for both countries.[1] Predicated on the India-France Road map on Cybersecurity and Digital Technology adopted in 2019, both countries are pursuing bilateral cooperation on advanced digital technologies, particularly in supercomputing, cloud computing, Artificial Intelligence, and quantum technologies, including the framework of the Global Partnership on Artificial Intelligence (GPIA). Both countries also reaffirmed the role of bilateral cyber dialogues in deepening cyber cooperation. There was also a broader agreement on exchanging best practices, information, evolving national cybersecurity strategy views, and developments in the cyber threat landscape.

Data leak from Bangladesh's government website

In a massive data leak in Bangladesh, a government website leaked the personal information of citizens, including full names, phone numbers, email addresses, and national ID numbers.[2] According to reports, the leak was accidentally discovered by a security researcher, following which he contacted the Bangladeshi e-Government Computer Incident Response Team (CIRT). The leak included data of millions of Bangladeshi citizens; however, the name of the website was not revealed to the public.

New EU-US data transfer pact

The European Commission announced a new data transfer pact with the United States regarding the transfer of personal data across the Atlantic.[3] According to the new EU-US Data Privacy Framework, the US is expected to ensure adequate protection for personal data transferred from the EU to the US companies.[4] The new framework also introduces new binding safeguards to address all concerns raised by the European Court of Justice, including the limiting access to EU data by US intelligence services. It also introduces significant improvements compared to the mechanism that existed under the privacy shield. The efficacy of the framework will be subjected to periodic reviews to be carried out by the European Commission, together with European data protection authorities and relevant US authorities.

Norway government websites hit by cyberattacks

There were reports of cyberattacks against Norwegian government ministries, which was largely due to vulnerability in the platform of one of the suppliers.[5] A police investigation is already underway, and the Norwegian Data Protection Authority was notified of the problem.[6] The attack is of unknown origin and has yet to be attributed to a threat actor. The cyber attack affected 12 government ministries, following which employees lost access to common mobile

services including e-mail. The Prime Minister's services, defense, foreign affairs, and justice ministries were not impacted as they have their separate platforms.

Kenyan government platforms suffer cybersecurity breach

The Kenyan government has officially confirmed that the eCitizen portal, utilized by the public to access more than 5,000 government services, was subjected to a cyber-attack.[7] The confirmation came in response to numerous complaints from citizens who encountered difficulties while using the portal for various services, including passport applications and renewals, issuance of e-visas for foreign visitors, obtaining driving licenses, identification cards, and national health records.

The confirmation of the cyber-attack was made by Eliud Owalo, the Minister of Information, Communication, and Digital Economy. He emphasized that despite the hackers' claim of stealing passport data, no actual data had been accessed or lost during the attack. The responsibility for the cyber-attack was claimed by a group identifying itself as "Anonymous Sudan," which presents itself as a collective of Sudanese cyber-warriors. This group has issued threats to retaliate against any attempts to meddle in Sudan's internal matters. However, there are suspicions that the group may have connections to Russia.

Cyberattack against Japan's biggest port

The Port of Nagoya, which is Japan's largest port in terms of total cargo throughput and plays a crucial role in handling Toyota Motor's car exports, suffered a severe cyberattack.[8] The same day, the port located in central Japan continued to experience difficulties loading and unloading containers from trailers. In response to the situation, the police have initiated an investigation as the port operator reported receiving a ransom demand to restore its system. According to the Nagoya Port Authority, the system failure originated when an employee encountered an issue in starting a computer. According to reports, the Russia-based ransomware group Lockbit 3.0 was responsible for the breach.

US FBI director warns of threat from China and AI

Keeping up sustained pressure on China, FBI Director Christopher Wray speaking at the bureau's Atlanta Cyber Threat Summit at the Georgia Tech Research Institute warned about the growing cyber threats to the US, while China has developed an ability to weaponize data with the advent of AI-related operations.[9] The director called China unparalleled among foreign adversaries and how the volume of personal and corporate data stolen by China in conjunction with the power of AI amplifies the challenges. He also emphasized that China possesses a significantly larger hacking program compared to the combined efforts of other countries. Sharing concerns about China's growing operational scale, and widening chasm between China-US, the director observed that "cyber hackers from China would still outnumber FBI cyber personnel by at least 50 to 1."[10] The director had shared a similar warning about Chinese hackers

outnumbering FBI cyber staff before a congress subcommittee in April 2023.[11]

Foreign spyware firms blacklisted by the US

The U.S. government took action by including four foreign commercial spyware entities on the Entity List.[12] The decision was made due to their involvement in activities that were deemed detrimental to the national security and foreign policy interests of the United States. The entities added to the Entity List are Intellexa S.A. in Greece, Intellexa Limited in Ireland, Cytrox AD in North Macedonia, and Cytrox Holdings Crt in Hungary. The government's determination was based on evidence that these companies engaged in the trafficking of cyber exploits, which were utilized to illicitly gain access to information systems. This unlawful activity posed a significant threat to the privacy and security of individuals and organizations on a global scale.

Once placed on the Entity List, companies intending to conduct business in the United States are obligated to adhere to stringent licensing prerequisites and other regulations to enhance supervision of their activities.[13] According to a press release from the agency, Intellexa and Cytrox will now encounter challenges in accessing commodities, software, and technology essential for the development of their surveillance tools.

Chinese hackers target U.S. officials

In a recent Chinese hacking attack that surprised Washington with its sophistication, the US ambassador to Beijing, Nicholas Burns, was reportedly among the American officials whose emails were accessed.[14] According to reports, another target of the attack was Daniel Kritenbrink, the Assistant Secretary of State for East Asia. Furthermore, the email account of the Commerce Secretary, Gina Raimondo, was also compromised, as disclosed by the administration. According to US officials, these were the three most senior targets, but the breach could have affected hundreds of thousands of government email accounts. The sensitivity of the breach is yet to be ascertained by the US government. The attack, reportedly exploited a flaw in Microsoft's cloud computing environment, which has since been fixed.

India File

- The Reserve Bank of India (RBI) has imposed a penalty of 65 lakh rupees on AP Mahesh Cooperative Urban Bank (APMCUB) for its failure to comply with the Cyber Security Framework for Primary Urban Cooperative Banks.[15] In 2022, hackers breached the security systems of APMCUB and siphoned off 12.48 crore, which the police investigation later revealed, occurred because of the bank's alleged negligence in implementing cybersecurity measures. According to the RBI guidelines, a bank should have security measures like anti-phishing application, intrusion prevention and detection systems, real-time threat defense, and management systems.

- In a massive data breach, over 12 thousand confidential records were leaked through Telegram channels, reportedly linked to the SBI account holders and employees.[16] The leaked information included screenshots of the SBI passbook, Aadhaar card, and voter card. The threat actor behind the incident has claimed to have exploited an unprotected database, granting access to the financial details of millions of consumers, like bank balances and recent transactions. The leaked data was also put up for sale in some of the dark web forums by some of these threat actors.

- According to a recently published IBM report, the average cost of data breach in India reached Rs. 17.9 crore in 2023, which is a 28 percent increase since 2020.[17] The detection and escalation costs in the country surged by 45 percent since 2020, constituting the largest portion of breach expenses. According to the report, the most prevalent causes of data breaches in India were phishing followed by compromised credentials. The report also stated that AI and automation have helped cut down the speed of breach identification and containment.

- In order to foster collaboration in the field of AI and emerging technologies, India AI, an independent business unit under Digital India Cooperation (DIC), Ministry of Electronics and Information Technology (MeitY) and Meta have signed an MoU.[18] The objective behind the move is to establish a framework for collaboration and cooperation including to make Meta's open-source AI models available for use by Indian AI ecosystem. The collaboration will make use of Meta's AI research models such as LlaMA, Massively Multilingual Speech, and No Language Left Behind. The primary focus of this partnership will revolve around creating datasets in Indian languages that facilitate translation and development of large language models, with special attention given to low-resource languages.

- The Ministry of Home Affairs organised a Conference on Crime & Security in the age of NFTs, AI and Metaverse under the banner of G-20 from 13-14 July 2023. A Chair's Summary was released under Indian Presidency.[19]

- India participated in the Fifth Substantive Session of UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) 2021-2025 which was held at UN Headquarters New York from 24-28 July 2023. Constructive contributions were made to the discussions on various critical aspect of development of rules, norms and principles of responsible behaviour of States in cyberspace, data international law compatible to cyberspace, practical confidence building measures and international

cooperation in capacity building in the context of existing inequality in cyber preparedness among Member States. A Second Annual Progress Report was adopted in the Fifth Substantive Session, which marks concrete progress in taking forward the mandate of the OEWG till 2025.

[1] Government of India (GoI), Ministry of External Affairs (MEA), Horizon 2047: 25th Anniversary of the India-France Strategic Partnership, Towards A Century of India-France Relations, 14 July 2023, https://mea.gov.in/bilateral-documents.htm?dtl/36806/Horizon+2047+25th+Anniversary+of+the+IndiaFrance+Strategic+Partnership+Towards+A+Century+of+IndiaFrance+Relations

[2] Techcrunch, Bangladesh government website leaks citizens' personal data, 7 July 2023, https://techcrunch.com/2023/07/07/bangladesh-government-website-leaks-citizens-personal-data/.

[3] Reuter, EU seals new US data transfer pact, but challenge likely, 11 July 2023, https://www.reuters.com/technology/eu-announces-new-us-data-transfer-pact-challenge-ahead-2023-07-10/

[4] European Commission, Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows, 10 July 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

[5] Cybernews, Norway government hit by cyberattack, 24 July 2023, https://cybernews.com/news/norway-government-cyberattacks-ministries/

[6] Euronews, Norway government ministries hit by cyber attack, authorities say, 24 July 2023, https://www.euronews.com/next/2023/07/24/norway-government-ministries-hit-by-cyber-attack-authorities-say

[7] BBC, Kenya cyber-attack: Why is eCitizen down?, 29 July 2023, https://www.bbc.com/news/world-africa-66337573

[8] Nikkei Asia, Japan's biggest port, Nagoya, hit by suspected cyberattack, 5 July 2023, https://asia.nikkei.com/Business/Technology/Japan-s-biggest-port-Nagoya-hit-by-suspected-cyberattack

[9] Cyberscoop, Top FBI officials warn of 'unparalleled' threat from China and AI, 26 July 2023, https://cyberscoop.com/fbi-officials-cybersecurity-china-ai/.

[10] Federal Bureau of Investigation (FBI), Director Wray Addresses FBI Atlanta Cyber Threat Summit, 26 July 2023, https://www.fbi.gov/video-repository/wray-atlanta-cyber-threats-072623.mp4/view

[11] CNBC, Chinese hackers outnumber FBI cyber staff 50 to 1, bureau director says, 28 April 2023, https://www.cnbc.com/2023/04/28/chinese-hackers-outnumber-fbi-cyber-staff-50-to-1-director-wray-says.html

[12] US Department of State, The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities, 18 July 2023, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/

[13] The Record, Two more foreign spyware firms blacklisted by US, 18 July 2023, https://therecord.media/spyware-companies-commerce-department-entity-list-intellexa-cytrox

[14] The Guardian, US ambassador to Beijing targeted in Chinese cyber-attack – report, 20 July 2023, https://www.theguardian.com/us-news/2023/jul/20/ambassador-to-beijing-among-us-officials-hit-by-chinese-hackers.

[15] The Times of India, RBI slaps Rs 65 lakh penalty on bank for hacking breach, 2 July 2023, https://timesofindia.indiatimes.com/city/hyderabad/rbi-slaps-rs-65-lakh-penalty-on-bank-for-hacking-breach/articleshow/101425742.cms?from=mdr

[16] India Today, Over 12,000 SBI employee data leaked on Telegram channels, 11 July 2023, https://www.indiatoday.in/india/story/telegram-channels-leak-data-of-12-thousand-sbi-employees-ignored-some-red-flag-2405024-2023-07-11

[17] Deccan Herald, Average cost of data breach in India hits record high of Rs 17.9 crore in 2023: IBM study, 25 July 2023, https://www.deccanherald.com/business/business-news/average-cost-of-data-breach-in-india-hits-record-high-of-rs-179-crore-in-2023-ibm-study-1240653.html

[18] Press Information Bureau (PIB), 'India AI' and Meta, India sign MoU to foster advancements in AI & Emerging Technologies, 26 July 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1943049.

[19] MHA, Conference webpage https://cyberconference-g20india.mha.gov.in/