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

CYBER *Digest*

April 2024

- Global regulatory developments in AI
- Cyberattacks hit government departments in France
- NHS Scotland confirms Ransomware attack
- Nepal to establish National Cyber Security Center
- US budget proposal boosts cybersecurity funding
- China to block Intel and AMD chips in government computers
- US sanctions Chinese firm
- Backdoor in Linux uncovered
- India File

Global regulatory developments in AI

The European Union Parliament has approved the Artificial Intelligence Act, a legislative measure aimed to safeguard fundamental rights, democracy, the rule of law, and environmental sustainability from the potential risks posed by high-risk AI technologies. The Act also aims to foster innovation and solidify Europe's position as a frontrunner in the AI domain. This regulation imposes obligations on AI systems commensurate with their potential risks and level of impact.[1] The newly implemented regulations prohibit specific AI applications that pose a threat to citizens' rights. These include biometric categorization systems reliant on sensitive characteristics, as well as indiscriminate scraping of facial images from the internet or CCTV footage for the creation of facial recognition databases. Emotion recognition in workplace and educational settings, social scoring, predictive policing solely based on profiling individuals or assessing their characteristics, and AI designed to manipulate human behavior or exploit vulnerabilities will also be banned.

In another significant development, the UN General Assembly unanimously adopted a resolution on Artificial Intelligence.[2] The resolution aims to encourage the protection of personal data, monitor AI for risks, and safeguard human rights. Sponsored by the United States and co-sponsored by 123 countries, it received consensus support from all 193 UN member nations. The resolution also acknowledged the potential of AI systems to expedite and facilitate progress towards achieving the 17 Sustainable Development Goals. This marks the first instance where the Assembly has adopted a resolution on regulating the emerging field.

Cyberattacks hit government departments in France

Reports indicate that several government departments were targeted by cyberattacks of "unprecedented intensity."[3] As per the prime minister's office, the impact was mitigated, and access to some government websites was "re-established."[4]However, the authorities noted that the identities of threat actors were unclear despite Anonymous Sudan's claim over their Telegram channel. Following the detection of the attacks, teams from the interministerial digital affairs department DINUM and France's cybersecurity agency ANSSI were mobilised to continue fending off the attacks.

In another yet similar incident, the French governmental employment agency reported a cyberattack, during which hackers likely extracted information concerning 43 million individuals.[5] The compromised personal data includes first and last names, Social Security numbers, employment agency France Travail identifiers, email and postal addresses, and telephone numbers, as confirmed by the French data protection agency CNIL.

NHS Scotland confirms Ransomware attack

A ransomware group is issuing threats to release a large volume of stolen data following a cyberattack on a Scottish health board.[6] NHS Dumfries and Galloway had cautioned in March that hackers might have gained access to substantial amounts of patient and staff data. Identified as INC

Ransom, the group has now declared its intention to publicly disclose three terabytes of data unless its demand for money is met. The cybercriminals have already released what they term a "proof pack," containing confidential information concerning a limited number of patients.

Nepal to establish National Cyber Security Center

The Nepalese government has decided to establish the National Cyber Security Center in alignment with the objectives outlined in the 'Digital Nepal Framework 2076 BS'.[7] The Council of Ministers, in a meeting held in January this year, made the decision to establish the center. The Ministry of Communication and Information Technology will spearhead the establishment of the Center, which will serve as a hub for digital forensic investigations and research and development in cybersecurity. It will also focus on promoting cybersecurity, enhancing public awareness, identifying challenges, and implementing measures for prevention, response, and recovery from cyber threats.

US budget proposal boosts cybersecurity funding

President Joe Biden's budget proposal for fiscal year 2025 calls for $13 billion in cybersecurity funding for civilian agencies.[8] This allocation includes additional investments aimed at enhancing digital defenses within the Departments of Justice, Homeland Security, and Health and Human Services, as revealed by the White House in March. Although the budget necessitates congressional approval to be enacted, it serves as an indicator of the administration's emphasis on cybersecurity preparedness. As per the proposal, the Cybersecurity and Infrastructure Security Agency (CISA) would receive an additional $103 million to strengthen defenses against hackers targeting federal and civilian networks. Furthermore, the agency would be allocated $470 million to implement network tools such as endpoint detection and response capabilities for federal assets.

China to block Intel and AMD chips in government computers

China, in new procurement guidelines, is looking to ban Intel and AMD chips in government computers and systems, according to a report.[9] The guidelines also seek to sideline Microsoft's Windows operating system and foreign-based database software in favor of Chinese solutions. The procurement guidelines, introduced last year, are currently being implemented. This action coincides with China's efforts to bolster its domestic semiconductor industry, aiming to decrease dependence on foreign technology. Semiconductors have become focal points in the technology rivalry between the U.S. and China in recent years.

US sanctions Chinese firm

The US imposed sanctions on a China-based firm, alleging it to be a front company for the Ministry of State Security.[10] The accusation suggests that the firm has been involved in numerous malicious cyber operations, specifically targeting critical infrastructure within the United States. The U.S. Treasury Department issued a statement detailing the sanctions imposed on Wuhan Xiaoruizhi Science and Technology, along with two Chinese

individuals. These actions were taken in collaboration with the U.S. Justice Department, FBI, State Department, and the United Kingdom as part of a coordinated effort. The Treasury emphasized that China state-sponsored malicious cyber actors continue to pose one of the most significant and enduring threats to U.S. national security.

Backdoor in Linux uncovered

It was reported that a malicious backdoor discovered within the extensively used data compression software library xz might potentially exist within instances of Fedora Linux 40 and the Fedora Rawhide developer distribution.[11] This form of authentication interference has the potential to enable an unauthorized individual to gain remote access to an affected system. A software engineer at Microsoft reportedly discovered a hidden backdoor within the Linux operating system when he observed an anomaly in the SSH application, typically used for remote computer access, consuming excessive processing power.[12] This anomaly led him to investigate a set of data compression tools known as xz Utils, suspecting a connection to previous errors. The presence of this backdoor raised concerns about a potential precursor to a major cyberattack, which experts believe could have inflicted extensive damage if successful.

India File

- In a proactive step to enhance the cyber defense capabilities of the Indian Armed Forces, the Defence Cyber Agency (DCyA) conducted the Chief Information Security Officers (CISO) Conclave – 24.[13] This two-day event, which took place on March 14th and 15th, 2024, gathered officers from the tri-services of the Indian Armed Forces under the oversight of Headquarters Integrated Defence Staff (HQ_IDS). A notable feature of the event was the execution of situation-based Table Top Exercises (TTX), designed to practice incident response protocols. These exercises, facilitated by the Data Security Council of India (DSCI), replicated genuine cyber threats and scenarios, allowing participants to evaluate their readiness and collaboration in effectively managing cyber incidents.

- According to reports, the Indian Army has established an elite unit called the Signals Technology Evaluation and Adaptation Group (STEAG), tasked with researching and evaluating futuristic communication technologies such as 6G, Artificial Intelligence (AI), Machine Learning (ML), and quantum computing for military applications, given the evolving nature of the field.[14] Officials stated that STEAG is entrusted with fostering technologies encompassing the entire spectrum of wired and wireless systems. The creation of STEAG is a strategic move by the Army to develop technologies in anticipation of future battlefield requirements.

- In alignment with the vision of "Making AI in India" and "Making AI Work for India," the Cabinet chaired by Prime Minister Shri Narendra Modi has endorsed the comprehensive national-level IndiaAI mission. This mission has been allocated a budget

outlay of Rs. 10,371.92 crore.[15]The mission aims to establish a comprehensive ecosystem aimed at catalyzing AI innovation. This will be achieved through strategic programs and partnerships spanning across both the public and private sectors.

[1] European Parliament News, Artificial Intelligence Act: MEPs adopt landmark law, 13 March 2024, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

[2] UN News, General Assembly adopts landmark resolution on artificial intelligence, 21 March 2024, https://news.un.org/en/story/2024/03/1147831

[3] Reuters, French state hit by cyberattacks of "unprecedented intensity" - media reports, 11 March 2024, https://www.reuters.com/technology/cybersecurity/french-state-hit-by-cyberattacks-unprecedented-intensity-media-reports-2024-03-11/

[4] Politico, French government hit with cyberattacks of 'unprecedented' intensity, 11 March 2024, https://www.politico.eu/article/french-government-hit-with-cyberattacks-of-unprecedented-intensity/

[5] Cybernews, Massive cyberattack affects 43 million French workers, 14 March 2024, https://cybernews.com/news/massive-cyberattack-affects-43-million-french-workers/

[6] BBC, Hackers threaten to publish huge cache of NHS data, 28 March 2024, https://www.bbc.com/news/articles/c3g5r9g45n4o

[7] The Annapurna Express, Government establishing National Cyber Security Center, 27 March 2024, https://theannapurnaexpress.com/story/48131/

[8] Cyberscoop, Biden's budget proposal seeks funding boost for cybersecurity, 11 March 2024, https://cyberscoop.com/biden-budget-cyber-2025.

[9] CNBC, China's new guidelines block Intel and AMD chips in government computers: FT, 24 March 2024, https://www.cnbc.com/2024/03/25/chinas-new-guidelines-will-block-intel-and-amd-chips-in-government-computers-ft.html.

[10] The Economic Times, US sanctions Chinese cyberespionage firm, saying it hacked US energy industry, 25 March 2024, https://economictimes.indiatimes.com/news/international/business/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry/articleshow/108770386.cms?from=mdr

[11] The Register, Malicious SSH backdoor sneaks into xz, Linux world's data compression library, 29 March 2024, https://www.theregister.com/2024/03/29/malicious_backdoor_xz/

[12] The New York Times, Did one guy just stop a huge cyberattack?, 3 April 2024, https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html

[13] SSB Crack, Defence Cyber Agency Hosts Chief Information Security Officers Conclave, 16 March 2024, https://www.ssbcrack.com/2024/03/defence-cyber-agency-hosts-chief-information-security-officers-conclave.html.

[14] The Hindu, Army raises elite unit to work on critical technologies having military applications, 18 March 2024, https://www.thehindu.com/news/national/army-raises-elite-unit-to-work-on-critical-technologies-having-military-applications/article67964387.ece.

[15] Press Information Bureau (PIB), Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem, 7 March 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2012357