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

CYBER *Digest*

December 2023

- **The Bletchley Declaration on AI Safety**
- **Nepal bans TikTok**
- **Australian Cybersecurity strategy 2023-2030 released**
- **Tri-Nation Mechanism to Counter North Korea's Cyber Threats**
- **Ransomware incidents around the world**
- **Data breaches impact companies worldwide**
- **India File**

The Bletchley Declaration on AI Safety

The United Kingdom hosted the first international AI Safety Summit to boost global efforts to cooperate on artificial intelligence (AI) safety. The declaration, by 28 countries and the European Union, was published on the opening day of the AI Safety Summit hosted at Bletchley Park, central England.[1] The summit's agenda centred on identifying mutual AI safety risks, establishing a collective scientific and evidence-based comprehension of these risks, and sustaining the understanding as AI capabilities advance. This was considered within the broader framework of a global approach aimed at comprehending the impact of AI on our societies.[2]

Another aspect was formulating individual risk-based policies within the participant countries to guarantee safety in response to these risks. Collaboration was encouraged while acknowledging that approaches might vary depending on national circumstances and relevant legal frameworks. This encompassed, in addition to heightened transparency by private entities advancing cutting-edge AI capabilities, the development of suitable evaluation metrics, tools for safety testing, and the enhancement of pertinent public sector capabilities and scientific research.

Nepal bans TikTok

Nepal has recently prohibited the Chinese-owned app TikTok, citing concerns that its content is "detrimental to social harmony".[3] This move follows the introduction of a new rule in the country, compelling social media companies to establish liaison offices within its borders. TikTok, boasting approximately a billion monthly users, has faced bans in various nations, including India. The decision by Nepal to ban the app reflects a broader global trend where concerns about content and potential societal impacts have led to regulatory actions against popular social media platforms. The Nepal administration's decision to ban TikTok was prompted by concerns over the platform spreading malicious content. Opposition leaders, on the other hand contend, that the ban was for political purposes and to suppress "dissent and gloss over governance failures."[4]

Australian Cybersecurity strategy 2023-2030 released

The 2023-2030 Australian Cyber Security Strategy delineates measures through which the Australian government and its agencies aim to enhance protection for themselves, individuals, and businesses against cyber criminals. Australia plans to strengthen its cybersecurity efforts by implementing a ransomware playbook for companies and attracting migrants with cyber expertise, as outlined in a new federal government plan. Under the $586 million plan, the government is dedicated to enhancing infrastructure protection and allocating funds for cyber awareness programs to provide better education for the population. After receiving numerous submissions from businesses and stakeholders, the government has announced its consideration of developing a single reporting portal. This initiative aims to simplify the process for businesses to report cyber incidents.

Tri-Nation Mechanism to Counter North Korea's Cyber Threats

The office of the South Korean president announced that the United States, South

Korea, and Japan have opted to create a high-level consultative body focused on cyber issues, primarily aimed at addressing North Korea's cyber activities.[5] The body has chosen to convene quarterly to enhance practical joint response capabilities to address global cyber threats. The announcement comes after the three countries' leaders agreed at a summit in August at Camp David to establish a new trilateral working group specifically focused on addressing cyber threats emanating from North Korea. This decision arises in the context of North Korea utilizing cyberattacks to procure funds for its nuclear and missile programs. According to a United Nations report, the North escalated its cryptocurrency theft in the past year, employing advanced techniques to surpass theft levels recorded in any other year, especially in 2022.

Ransomware incidents around the world

According to reports, internal data from Boeing, one of the world's largest defence and space contractors, has been released online by Lockbit, a cybercrime gang known for extorting victims by stealing and disclosing data unless a ransom is paid.[6] As per reports, the company acknowledged disruptions in its operations resulting from cyber incidents. Boeing asserted its confidence that the event does not threaten aircraft or flight safety. However, the company refrained from commenting on whether Lockbit had obtained defence or other sensitive data. In a separate incident, the U.S. unit of the Industrial and Commercial Bank of China (ICBC) Financial Services, the largest commercial lender in China by assets, reported an ongoing investigation into an attack that disrupted some of its systems. The company also mentioned making progress toward recovering from the incident.[7]

Reports indicate that India's premier state-owned aerospace research organization, the National Aerospace Laboratories, has allegedly been compromised by the LockBit ransomware operation. According to reports, LockBit posted confidential letters, internal documents, and an employee passport on its data leak site. The group issued a warning that if the National Aerospace Laboratories (NAL) fails to meet their unspecified ransom demand, all stolen data from NAL will be exposed. As of now, neither NAL nor India's Computer Emergency Response Team has officially confirmed the claims of a ransomware attack.

Data breaches impact companies worldwide

Reports suggest that the personal information of approximately 1.5 million people may have been exposed in a data breach at the Taj Hotels group, owned by Tata. The threat actor using the alias “Dnacookies,” identified as a threat actor, has demanded $5,000 for the complete dataset. This dataset comprises addresses, membership IDs, mobile numbers, and other personally identifiable information (PII), as reported by individuals familiar with the situation. In a post on BreachForums, the threat actor claimed that the customer data covers the period from 2014 to 2020 and has not been shared with any party thus far. Furthermore, the individual specified three conditions for any potential deal.

According to reports, Gulf Air, Bahrain's flag carrier, has revealed that it was affected

by a data breach, potentially resulting in the exposure of specific email and client database information. Acknowledging the breach, Gulf Air stated that the unauthorized access to systems prompted the immediate implementation of contingency plans. While the airline did not provide specific details about the incident, it emphasized that operations and critical systems have not been affected. The Gulf Air breach occurred against the backdrop of a rising prevalence of data compromises, with threat actors consistently employing innovative methods to access and exfiltrate sensitive information illicitly.

DP World Australia limited access to its Australian port operations in Brisbane, Melbourne, and Sydney following the detection of a cyber incident.[8] It is the country's second-largest port operator, managing nearly 40% of the goods entering and leaving Australia. The incident was made public when the port operator notified the Australian government. Subsequently, it became known that data of employees had been stolen with client data remaining secure.[9]

India File

- Expert Group Meeting of the Shanghai Cooperation Organisation (SCO) Member States on International Information Security (IIS) was held in Beijing from 15-17 November 2023 in hybrid mode. Indian delegation participated in this three-day event in virtual mode.
- The Ministry of Electronics and Information Technology (MeitY) has issued blocking orders against 22 illegal betting apps and websites. The move comes in response to investigations carried out by the Enforcement Directorate (ED) into an illegal betting app syndicate.[10]
- A cryptocurrency scam in Himachal Pradesh, India, amounting to Rs 2500 crore, has impacted approximately 5,000 government employees and individuals who had received compensation for their land.[11] Continuing its crackdown against the scam, the special police team (SIT) has nabbed eight more persons, taking the arrests to 18. The SIT has reconstructed the website involved in the crypto scam having almost 2.5 lakh different IDs.
- The Central government has included the Computer Emergency Response Team (CERT-In) in a list of organizations that are exempted from the scope of the Right to Information Act (RTI), 2005.[12] As the national nodal agency for responding to computer security incidents, CERT-In plays a crucial role in addressing such incidents as they arise. Operating under the Ministry of Electronics and Information Technology, CERT-In joins a list of 26 other intelligence and security organizations established by the Central government which are already exempted under the Right to Information Act (RTI).

[1] Reuters, Britain publishes 'Bletchley Declaration' on AI safety, 1 November 2023, https://www.reuters.com/technology/britain-publishes-bletchley-declaration-ai-safety-2023-11-01/

[2] Government of UK, The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023, 1 November 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

[3] BBC, Nepal bans TikTok citing disruption to social harmony, 14 November 2023, https://www.bbc.com/news/business-67411535

[4] The Hindu, In Nepal's TikTok ban there's more than meets the eye, 21 November 2023, https://www.thehindu.com/news/international/in-nepals-tiktok-ban-theres-is-more-than-meets-the-eye/article67554683.ece

[5] The Record, US, South Korea and Japan launch group to tackle North Korea hacking, 6 November 2023, https://therecord.media/south-korea-japan-us-cyberthreat-body-north-korea-hacking

[6] Reuters, Boeing data published by Lockbit hacking gang, 11 November 2023, https://www.reuters.com/technology/cybersecurity/boeing-data-published-by-lockbit-hacking-gang-2023-11-10/

[7] Reuters, China's biggest lender ICBC hit by ransomware attack, 10 November 2023, https://www.reuters.com/world/china/chinas-largest-bank-icbc-hit-by-ransomware-software-ft-2023-11-09/

[8] CSO, Major Australian ports shut down following cyber incident, 12 November 2023, https://www.csoonline.com/article/1246710/major-australian-ports-shut-down-following-cyber-incident.html

[9] Reuters, DP World says hackers stole Australian ports employee data, 28 November 2023, https://www.reuters.com/technology/cybersecurity/dp-world-says-hackers-stole-australian-ports-employee-data-2023-11-28/

[10] Press Information Bureau (PIB), MEITY issues blocking orders against 22 illegal betting apps & websites, 5 November 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1974901

[11] The Times of India, ₹2.5k cr cryptocurrency scam: 4 cops among 8 more arrested, 6 November 2023, https://timesofindia.indiatimes.com/city/shimla/2-5k-cr-cryptocurrency-scam-4-cops-among-8-more-arrested/articleshow/104997746.cms

[12] The Hindu, Central government exempts CERT-In from RTI Act, 24 November 2023, https://www.thehindu.com/news/national/central-government-exempts-cert-in-from-rti-act/article67569804.ece