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

CYBER *Digest*

February 2025

- UK mulls more measures to strengthen cybersecurity
- UN aviation agency reports cyber incident
- Luxembourg government websites taken offline in a cyberattack
- Cyberattacks target Israeli kindergartens
- Pro-Ukrainian threat actors hack Russian ISP
- Swiss banks and councils targeted during annual WEF meeting
- DeepSeek Hit by Cyberattacks
- UN Security Council discusses commercial spyware threat
- Pakistan moves to regulate social media
- Turkiye's cybersecurity bill sparks human rights concerns
- TikTok faces nationwide ban in the US
- India File

UK mulls more measures to strengthen cybersecurity

The UK government has taken the initiative to criminalize the creation and distribution of sexually explicit deepfake images.[1] This move aims to combat the rising spread of such content, which primarily targets women and girls. While Britain outlawed the sharing of intimate photos or videos without consent, commonly known as revenge porn, in 2015, the existing legislation does not address fake images.

The UK government is also considering a ban on all public bodies from making ransomware payments as part of efforts to combat cyber threats.[2] Under the plan, critical national infrastructure operators will be prohibited from complying with ransom demands when hackers seize IT systems. Private companies will be required to report such payments to the government, with transactions potentially blocked if they involve sanctioned entities or foreign states. If enacted, the proposals will also make reporting ransomware attacks mandatory.

UN aviation agency reports cyber incident

The UN's civil aviation agency, the International Civil Aviation Organization (ICAO), is investigating a possible security breach after a hacker forum claimed that 42,000 records were stolen.[3] ICAO stated that the incident was limited to its recruitment systems and did not impact aviation safety or security operations.[4] The threat actor, known as Natohub, operates on BreachForums 2, a successor to a site seized by the FBI in 2023. Registered six months ago, the account previously claimed to have accessed the personal data of 14,000 UN delegates.

Luxembourg government websites taken offline in a cyberattack

The State Information Technology Centre (CTIE) confirmed that a cyberattack hit several Luxembourg government websites.[5] The MyGuichet portal and LuxTrust digital identity service were both offline for about two hours due to a Distributed Denial-of-Service (DDoS) attack. MyGuichet.lu is the official online administrative portal for citizens in Luxembourg, while LuxTrust is a leading provider of secure digital identity and authentication solutions in the country. The services were eventually restored. Just a week after this incident, customers trying to access bank accounts or other personal services faced issues as LuxTrust was targeted by a cyberattack for the second time in less than a week.[6] The company confirmed that its services were unavailable for about 30 minutes due to a DDoS attack.

Cyberattacks target Israeli kindergartens

According to reports, hackers breached the panic button system of Maagar-Tec, triggering sirens and broadcasting pro-terrorism messages in around 20 kindergartens, according to the National Cyber Directorate.[7] The hackers also sent threatening text messages to tens of thousands of citizens after compromising another system. The Iranian-affiliated hacker group Handala has claimed responsibility for the attack. The hackers claimed to have breached Maagar-Tec, an Israeli electronics firm responsible for panic button systems in schools.[8] The company informed local media that it had disconnected the affected systems and was investigating the breach.

Pro-Ukrainian threat actors hack Russian ISP

Russian internet provider Nodex announced it was working to restore its systems following a cyberattack that compromised its network and wiped internal servers, leading to a complete loss of internet connectivity for its Russian customers.[9] The company later attributed the cyberattack to Ukrainian hackers, claiming it led to a "complete failure" of its infrastructure.[10] The hacking group Ukrainian Cyber Alliance took responsibility for the attack, sharing screenshots from key servers within Nodex's network.

Swiss banks and councils targeted during annual WEF meeting

During the annual World Economic Forum (WEF), Russian hackers have reportedly launched cyberattacks on Swiss institutions.[11] According to the Swiss news agency ATS, the attacks targeted regional banks and local councils, sparking widespread concern across Switzerland. The NCSC has attributed the attack to the Russian hacker group "NoName" as responsible for the attacks. Known for its disruptive cyber activities, the group carried out a DDoS attack, flooding websites and applications with excessive traffic to make them inaccessible to users.

DeepSeek Hit by Cyberattacks

DeepSeek confirmed that large-scale malicious attacks on its services prompted the company to restrict user registrations temporarily.[12] It reported multiple waves of DDoS attacks targeting its API and chat system interfaces since the release of its large language models on January 20. Chinese state media reported that the cyberattack originated in the US.[13] Other independent reports noted that the top three sources of the attack infrastructure were the U.S. (20%), the U.K. (17%), and Australia (9%).[14] The Chinese AI startup recently surpassed OpenAI's ChatGPT to become the most downloaded free app in Apple's App Store and Google Play store ion over 140 countries.

UN Security Council discusses commercial spyware threat

For the first time, UN Security Council members met to discuss the threat of commercial spyware.[15] At the informal Arria-formula meeting, a senior US diplomat urged stronger efforts to secure justice for victims, while other nations pledged action. The discussion comes amid growing concerns over spyware infecting diplomats' devices. China and Russia opposed the US-led hearing, with China emphasizing the need to focus on nation-state cyberweapons like the Stuxnet virus used against Iran's nuclear program. Russia called for a broader UN discussion on spyware.

Pakistan moves to regulate social media

Pakistan's opposition expressed concerns over the government's proposed social media controls, fearing it would further suppress freedom of speech.[16] The proposal includes blocking platforms and imprisoning users for spreading disinformation. The Prevention of Electronic Crimes Act, introduced by Pakistan's Law Minister, would establish an agency with the authority to block "unlawful and offensive content" on social media and ban individuals or organizations.[17] Social media platforms would be required to register with the new Social Media Protection and Regulatory Authority, facing potential temporary or permanent bans for non-compliance. The law also criminalizes the spread of disinformation, with penalties including up to three years in prison and a fine of 2 million rupees (USD 7,150).

Turkiye's cybersecurity bill sparks human rights concerns

A newly introduced cybersecurity bill in the Turkish Parliament has faced strong criticism, with concerns raised about potential threats to human rights and personal freedoms.[18] While the bill seeks to strengthen the country's defenses against rising cyber threats, it has raised alarms over surveillance, data privacy, and the consolidation of power within government institutions. The bill is expected to be fast-tracked to establish a legal framework for the Cybersecurity Directorate, created by President Recep Tayyip Erdogan on January 8. The proposed legislation grants broad powers to the newly established directorate, including the authority to collect and store extensive data from public institutions and critical infrastructure providers

TikTok faces nationwide ban in the US

TikTok has officially shut down in the United States as a federal ban took effect on January 19, 2025.[19] As a result, existing users can no longer access TikTok content, while new users are unable to download the app from official Android and iOS stores. Other ByteDance-owned apps, including CapCut, Lemon8, and Gauth, have also been removed. The ban follows a unanimous US Supreme Court ruling upholding a law that required ByteDance to either sell TikTok or face a nationwide block due to national security concerns and fears that its recommendation algorithm could be influenced by Chinese authorities.

Later, US President Donald Trump issued an executive order granting TikTok a 75 day extension to comply with the ban unless sold.[20] However, the order does not lift the ban but directs the attorney general to delay enforcement.

India File

- Between January 1 and November 15, 2024, there were 92,323 reported cases of digital arrest scams nationwide, with a total amount defrauded of Rs. 2,140.99 crore. In the latest such instance, a bank manager at the State Bank of India (SBI) in central Delhi stopped a 68-year-old retired school teacher from falling victim to a digital arrest scam.[21] The teacher was about to transfer Rs. 79 lakh to the scammer.

- The Ministry of Electronics and Information Technology (MeitY) held a consultation meeting with government officials and industry representatives on the Draft Digital Personal Data Protection (DPDP) Rules, 2025, providing a valuable opportunity to contribute to India's data protection framework before the public feedback deadline of February 18, 2025.[22] The session was attended by over 200 participants, including key government officials from various ministries, industry leaders, legal experts, and policymakers, to discuss the rules aimed at supporting the implementation of the Digital Personal Data Protection Act 2023.

- The ransomware group Bashe has claimed responsibility for breaching the database of ICICI Bank, one of India's top banking institutions.[23] According to information found on the dark web, the hackers have set a ransom deadline of January 24, 2025, to prevent the public release of sensitive data. They warned that failure to meet their demands would result in the exposure of the data. Subsequent reports indicated that the sample data shared as "proof" appeared incomplete and lacked credibility, raising questions about the authenticity of the claims and the true extent of the breach.[24]
- Tata Technologies Ltd. suspended some of its IT services following a ransomware attack that affected the company's network.[25] The company confirmed that the attack temporarily impacted IT assets, which have now been restored. Despite the cyberattack, client delivery services remained fully operational, with no disruption to customer operations.

[1] Reuters, Britain to make sexually explicit 'deepfakes' a crime, 7 January 2025, https://www.reuters.com/world/uk/britain-make-sexually-explicit-deepfakes-crime-2025-01-07/

[2] The Guardian, Ministers consider ban on all UK public bodies making ransomware payments, 14 January 2025, https://www.theguardian.com/technology/2025/jan/14/ministers-consider-ban-on-all-uk-public-bodies-making-ransomware-payments

[3] Reuters, UN aviation agency investigating reports of possible data breach, 7 January 2025, https://www.reuters.com/technology/cybersecurity/un-aviation-agency-investigating-reports-possible-data-breach-2025-01-06/

[4] The Record, UN aviation agency ICAO confirms its recruitment database was hacked, 8 January 2025, https://therecord.media/icao-un-confirms-recruitment-systems-data-breach

[5] Luxembourg Times, Luxembourg government websites knocked offline in latest cyberattack, 10 January 2025, https://www.luxtimes.lu/luxembourg/luxembourg-government-websites-knocked-offline-in-latest-cyberattack/33948495.html

[6] Luxembourg Times, LuxTrust targeted by yet another cyber attack, 15 January 2025, https://www.luxtimes.lu/luxembourg/luxtrust-identity-verification-service-under-attack-company-works-to-restore-services/34560282.html

[7] Calcalistech, Panic buttons in Israeli kindergartens hacked in cyberattack by Iran-affiliated group, 26 January 2025, https://www.calcalistech.com/ctechnews/article/bkgdbynukg

[8] The Record, Hackers hijack emergency sirens in kindergartens across Israel, 28 January 2025, https://therecord.media/hackers-hijack-sirens-iran-israel

[9] TechCrunch, Ukrainian hackers take credit for hacking Russian ISP that wiped out servers and caused internet outages, 8 January 2025, https://techcrunch.com/2025/01/08/ukrainian-hackers-take-credit-for-hacking-russian-isp-that-wiped-out-servers-and-caused-internet-outages/

[10] Ibid.

[11] The 420, Russian Hackers Target Swiss Banks and Local Councils Amid World Economic Forum, 23 January 2025, https://www.the420.in/russian-hackers-target-swiss-banks-during-wef/

[12] CNBC, DeepSeek hit with large-scale cyberattack, says it's limiting registrations, 27 January 2025, https://www.cnbc.com/2025/01/27/deepseek-hit-with-large-scale-cyberattack-says-its-limiting-registrations.html

[13] South China Morning Post , Cyberattack on DeepSeek, including brute-force assault, started in US: Chinese state media, 30 January 2025, https://www.scmp.com/news/china/politics/article/3296765/cyberattack-deepseek-including-brute-force-assault-started-us-chinese-state-media

[14] Techtarget, NSFocus: DeepSeek AI hit with 'well planned' DDoS attacks 3 February 2025 https://www.techtarget.com/searchsecurity/news/366618543/NSFocus-DeepSeek-AI-hit-with-well-planned-DDoS-attacks.

[15] The Record, UN Security Council members meet on spyware for first time, 15 January 2025, https://therecord.media/commercial-spyware-meeting-un-security-council-members

[16] Hindustan Times, Pakistan moves toward extensive social media regulation. Details here, 23 January 2025, https://www.hindustantimes.com/world-news/pakistan-moves-toward-extensive-social-media-regulation-details-here-101737628152823.html

[17] Ibid.

[18] Nordic Monitor, New cybersecurity bill would grant Erdogan gov't unrestricted control over personal data, 21 January 2025, https://nordicmonitor.com/2025/01/new-cybersecurity-law-grants-erdogan-govt-unrestricted-control-over-personal-data/

[19] The Hacker News, TikTok Goes Dark in the U.S. as Federal Ban Takes Effect January 19, 2025, 19 January 2025, https://thehackernews.com/2025/01/tiktok-goes-dark-in-us-as-federal-ban.html

[20] BBC, What does Trump's executive order mean for TikTok and who might buy it?, 22 January 2025, https://www.bbc.com/news/articles/clyng762q4eo

[21] The Hindu, Retired teacher saved from a digital arrest scam, thanks to bank staff, 14 January 2025, https://www.thehindu.com/news/national/sbi-manager-saves-68-year-old-retired-school-teacher-from-digital-arrest-scam/article69096275.ece.

[22] Press Information Bureau (PIB), MeitY organises consultation meeting of government officials and industry on the Draft Digital Personal Data Protection (DPDP) Rules, 2025, 14 January 2025, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2092928

[23] The 420, ICICI Bank Faces Potential Data Breach; Suspected Ransomware Group 'BASHE' Involved, 23 January 2025, https://www.the420.in/bashe-hacking-group-claims-icici-bank-data-breach-ransom-deadline-jan-24-2025/

[24] India Today, The breach that probably isn't: The 'alleged' ICICI Bank data leak, January 24, 2025 URL: https://www.indiatoday.in/india/story/icici-bank-data-leak-breach-probably-isnt-2669732-2025-01-24

[25] Bleeping Computer, Indian tech giant Tata Technologies hit by ransomware attack, 31 January 2025, https://www.bleepingcomputer.com/news/security/indian-tech-giant-tata-technologies-hit-by-ransomware-attack/