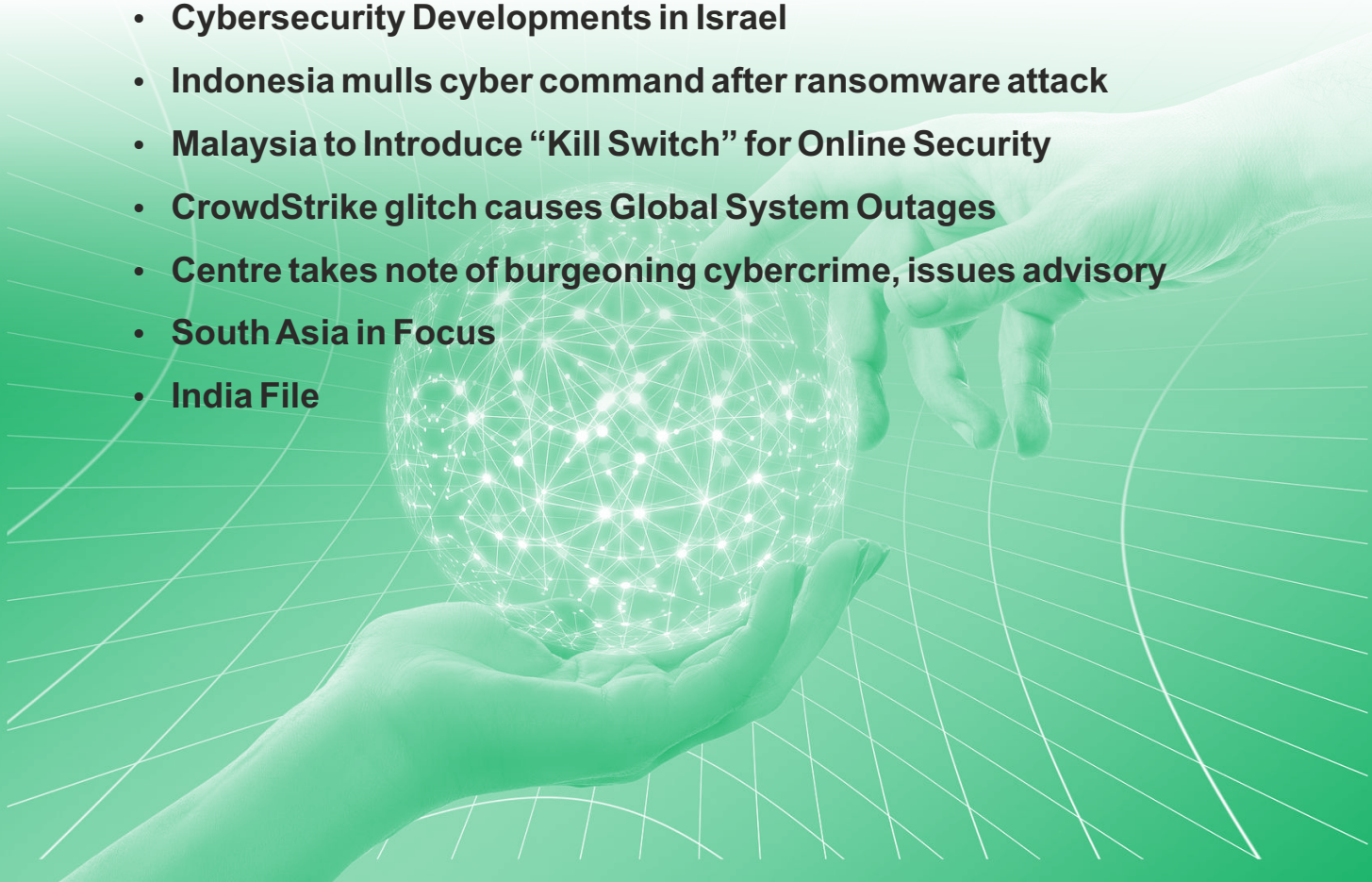
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

August 2024

- Germany Accuses China of 2021 Cyber Attack, Secures 5G Networks
- AT&T Data Breach Exposes Call and Text Records of Millions
- Europol's Operation Morpheus Targets Cobalt Strike Misuse
- Cybersecurity Developments in Israel
- Indonesia mulls cyber command after ransomware attack
- Malaysia to Introduce "Kill Switch" for Online Security
- CrowdStrike glitch causes Global System Outages
- Centre takes note of burgeoning cybercrime, issues advisory
- South Asia in Focus
- India File



Germany Accuses China of 2021 Cyber Attack, Secures 5G Networks

Germany has attributed a 2021 cyber attack on its precision mapping agency to China, suggesting the breach may have exposed sensitive information crucial for protecting critical infrastructure.[1] The German foreign office summoned the Chinese ambassador to Berlin to file a formal complaint. These conclusions follow a three-year investigation by German security authorities into the malware that compromised the Federal Office for Cartography and Geodesy (BKG).

Germany also announced it will ban critical components from Chinese companies Huawei and ZTE in key parts of its 5G networks.[2] According to Interior Minister Nancy Faeser, Huawei and ZTE components will be removed from 5G core networks by the end of 2026, and their critical management systems in 5G access and transport networks must be replaced by the end of 2029.

AT&T Data Breach Exposes Call and Text Records of Millions

AT&T has disclosed a massive data breach affecting tens of millions of its cellphone customers, as well as many non-AT&T customers.[3] The exposed data includes call and text message records from mid-to-late 2022, covering nearly all AT&T cellular customers and those of wireless providers using its network between May 1, 2022, and October 31, 2022.

The breach involved stolen logs detailing the phone numbers contacted by AT&T customers, the frequency of interactions, and the duration of calls. However, AT&T emphasized that the compromised data does not include the content of calls or text messages nor the specific timing of these communications.

Europol's Operation Morpheus Targets Cobalt Strike Misuse

Europol has announced a significant global initiative, termed Operation Morpheus, targeting the criminal misuse of Cobalt Strike, the commercial penetration testing tool widely used by cybersecurity testers to check for vulnerabilties.[4] The coordinated action resulted in the dismantling of 593 servers that were being used for illicit purposes. This operation marked a collaboration between law enforcement agencies and the private sector to address the exploitation of this legitimate red teaming tool, which criminals have been using to infiltrate victims' IT systems.[5]

Spearheaded by the U.K. National Crime Agency, the investigation involved law enforcement authorities from Australia, Canada, Germany, the Netherlands, Poland, and the United States. Europol played a key role in coordinating international efforts and facilitating communication with private partners.

Cybersecurity Developments in Israel

Since the outbreak of war between Israel and Hamas on October 7, the Israel Defense Forces' cloud computing network has been subjected to over three billion cyber attacks, according to the commander of the military's computer unit.[6] Despite the scale of the attacks, all were successfully intercepted without causing any damage. The targeted attacks focused on the

operational cloud computing systems used by troops to share critical information and locations.

In a notable incident, private data, including blood test results and login credentials of Israeli athletes, were released on Telegram in a doxing cyberattack, according to reports.[7] The hacker group, which identified itself as "Zeus," also disclosed personal information revealing the military status of the athletes on social media. The attack has been reported to Pharos, a division of France's Anti-Cybercrime Office (OFAC), which is investigating the breach.

Indonesia mulls cyber command after ransomware attack

Indonesia is starting to recover data encrypted during a significant ransomware attack last month that impacted over 160 government agencies.[8] The cyber attack caused disruptions across various government services, including immigration and operations at major airports. Officials have admitted that much of the affected data was not backed up, complicating the recovery efforts. Brain Cipher, the hacker group responsible for the recent breach of Indonesia's Temporary National Data Center (PDNS), has reportedly apologized for the attack and provided the government with an encryption key.[9]

There is increasing momentum in Jakarta for the Indonesian government to establish a separate military branch focused exclusively on cyber warfare. Former National Resilience Institute governor Andi Widjajanto has highlighted that the creation of this new branch is becoming an urgent necessity. Widjajanto noted that both state and non-state actors are demonstrating the capability to launch cyber attacks against the country. He stressed the importance for the government to act quickly on this proposal to enhance national cybersecurity.

Malaysia to Introduce "Kill Switch" for Online Security

Malaysia's government is preparing to implement a "kill switch" to bolster online security and address cybercrime.[10] Minister in the Prime Minister's Department (Law and Institutional Reform) Azalina Othman Said announced that the initiative is expected to be presented in Parliament during the upcoming October session. The proposed kill switch aims to enhance the accountability of social media and internet messaging platforms in tackling cybercrimes, including online scams, cyberbullying, child pornography, and sexual harassment.

CrowdStrike glitch causes Global System Outages

The cybersecurity company CrowdStrike caused widespread computer system outages worldwide, affecting various industries and creating chaos at airports, financial institutions, and healthcare systems.[11] The disruption stemmed from a faulty update to CrowdStrike Falcon, the company's popular endpoint detection and response (EDR) platform, which caused Windows machines to crash and enter an endless reboot cycle, leading to widespread server failures. As one of the leading cybersecurity firms, CrowdStrike's software is extensively used globally, with over half of Fortune 500 companies relying on their security products. Consequently,

the impact of the flawed update was significant, with some labelling it the "largest IT outage in history."

The Indian government's cybersecurity agency, CERT-In, has alerted that CrowdStrike users are being targeted by a phishing attack. The agency has detailed several tactics used in this campaign, including phishing emails that impersonate CrowdStrike support. The Indian government's cybersecurity agency, CERT-In, has alerted that CrowdStrike users are being targeted by a phishing attack.[12] The agency has detailed several tactics used in this campaign, including phishing emails that impersonate CrowdStrike support.

In a silver lining of sorts, the global IT outage led to the discovery of a major financial fraud at Manappuram Comptech & Consultants Ltd.[13] Dhanya Mohan, arrested for the alleged fraud, had spent five years concealing her actions while embezzling Rs 20 crore through the company's personal loan app. As an AGM Tech-lead, she used her position to delete records of her fraudulent transactions. The scheme unraveled due to the IT outage, wherein she couldn't erase the data, leading to the company investigating her transactions and uncovering the fraud. She had been using the money to fund her online rummy addiction.[14]

Centre takes note of burgeoning cybercrime, issues advisory

The cybercrime unit I4C, under the Union Ministry of Home Affairs (MHA), has advised the public to be wary of suspicious e-notices from government offices received via email.[15] They recommend verifying the authenticity of the official's name mentioned in the email by checking online and calling the relevant department to confirm its legitimacy. A similar alert was issued in May when the Union Ministry of Home Affairs (MHA) warned against 'blackmail' and 'digital arrests' by cybercriminals posing as police officers or representatives of central agencies like the Central Bureau of Investigation (CBI), the Enforcement Directorate (ED), and the Reserve Bank of India (RBI).[16] This organized online economic crime is believed to be operated by cross-border syndicates.

The Centre's senior inter-ministerial panel has pinpointed vulnerabilities in the banking, immigration, and telecom sectors that facilitate cyber scams from Southeast Asia.[17] Key issues identified include senior bank managers at two nationalized banks opening mule accounts; approximately 30,000 visitors to Cambodia, Thailand, Myanmar, and Vietnam from January 2022 to May 2024 who have not returned; and the misuse of bulk SIM cards.

South Asia in Focus

UAE Deports Eleven Sri Lankans for Cybercrime

Eleven Sri Lankan nationals have been deported from the United Arab Emirates (UAE) after being charged with cybercrimes.[18] The Sri Lanka Bureau of Foreign Employment (SLBFE) reported that UAE authorities have arrested a total of 37 individuals suspected of involvement in such activities. The SLBFE stated that these suspects will be deported within the next two weeks, pending the conclusion of ongoing investigations in the UAE. Upon receiving the UAE's investigation reports,

the SLBFE will work with the Ministry of Foreign Affairs and Sri Lankan Police to determine further actions for the deported individuals.

Pakistan deploying Chinese style - Internet Firewall

Pakistan's Minister for Information Technology and Telecommunication announced that the government is deploying an internet firewall as part of a cybersecurity upgrade, countering claims that it will suppress free speech.[19] The firewall is part of the country's broader Digital Infrastructure Development Initiative, which has received over $70 million in the latest budget. Critics and digital rights activists express concern that the firewall could be used to stifle dissent, especially as the Pakistani military faces significant online criticism regarding its alleged role in detaining former Prime Minister Imran Khan and cracking down on his party.

Internet shutdown in Bangladesh as protests escalate

The government short to control student protests in Bangladesh by shutting down mobile Internet services on July 17 to control the situation and counter fake news. Subsequently broadband Internet was also blocked and restored week later on a limited scale. Social media platforms like Facebook TikTok WhatsApp and YouTube remained blocked. Mobile Internet was resumed on July 28th and the restrictions on social media were lifted on July 31st.[20]

India File

- The Sixth Cyber Dialogue between India and the United Kingdom took place on July 3, 2024, in New Delhi.[21] The discussions covered topics such as cyber threat assessment, internet governance, data protection, critical infrastructure protection, capacity building, and cooperation in multilateral forums, including recent developments in the cyber realm at the United Nations. Both nations agreed to enhance cooperation between their cyber agencies to ensure a safe and robust cyberspace.
- The Union government confirmed a data breach in BSNL's systems, reported on May 20 by the Indian Computer Emergency Response Team (CERT-In).[22] Minister of State for Communications, Chandra Sekhar Pemmasani mentioned in a written response to a Lok Sabha query that although the breach did not cause any service outages, one BSNL server contained data similar to the sample provided by CERT-In. According to Dr. Pemmasani, an inter-ministerial committee has been established to audit telecom networks and recommend measures to prevent data breaches.
- WazirX, a leading Indian cryptocurrency exchange, experienced a major cyberattack in which hackers allegedly stole over $230 million—nearly half of the platform's reserves.[23] This breach underscores the security

risks facing cryptocurrency exchanges and their growing appeal as targets for global hackers. In response to the attack, the FBI has contacted Indian cryptocurrency exchange WazirX to investigate the cyberattack, which is reportedly linked to North Korean cybercriminals, and to offer assistance with the probe, according to reports.[24]

- A ransomware attack on C-Edge Technologies, a major banking tech provider in India, has led to the temporary shutdown of payment systems at nearly 300 small local banks.[25] In response, the National Payment Corporation of India (NPCI) is conducting a comprehensive audit to contain and prevent the spread of the attack.

[1] Financial Times, Germany blames China for 'serious' cyber attack, 31 July 2024, https://www.ft.com/content/6be7fcb7-0763-4021-a715-410e306d138f

[2] AP News, Germany to bar Chinese companies' components from core parts of its 5G networks, 11 July 2024, https://apnews.com/article/germany-china-huawei-zte-ban-5g-networks-fc969a68958f4a4b928ce0f8a1c32087.

[3] CNN, Nearly all AT&T cell customers' call and text records exposed in a massive breach, 12 July 2024, https://edition.cnn.com/2024/07/12/business/att-customers-massive-breach/index.html

[4] Industrial Cyber, Operation Morpheus: Europol leads global crackdown, dismantles 593 Criminal Cobalt Strike servers, 5 July 2024, https://industrialcyber.co/ransomware/operation-morpheus-europol-leads-global-crackdown-dismantles-593-criminal-cobalt-strike-servers.

[5] Ibid.

[6] The Times of Israel, IDF computer chief: 3 billion cyber attacks against Israel since beginning of war, 13 July 2024, https://www.timesofisrael.com/idf-computer-chief-3-billion-cyber-attacks-against-israel-since-beginning-of-war.

[7] The Times of Israel, French cybercrimes team called in after Israeli athletes' data leaked online, 28 July 2024, https://www.timesofisrael.com/french-cybercrimes-team-called-in-after-israeli-athletes-data-leaked-online/

[8] Reuters, Indonesia says it has begun recovering data after major ransomware attack, 12 July 2024, https://www.reuters.com/technology/cybersecurity/indonesia-says-it-has-begun-recovering-data-after-major-ransomware-attack-2024-07-12/

[9] The Register, Ransomware scum who hit Indonesian government apologizes, hands over encryption key, 4 July 2024, https://www.theregister.com/2024/07/04/hackers_of_indonesian_government_apologize/

[10]The Straits Times, Malaysia's government to introduce 'kill switch' to boost online security, 28 July 2024, https://www.straitstimes.com/asia/se-asia/malaysia-s-government-to-introduce-kill-switch-to-boost-digital-security

[11] CIO, CrowdStrike failure: What you need to know, 1 August 2024, https://www.cio.com/article/3476789/crowdstrike-failure-what-you-need-to-know.html

[12] India Today, After global Windows outage, Crowdstrike users now face phishing attacks, 29 July 2024, https://www.indiatoday.in/technology/news/story/after-global-windows-outage-crowdstrike-users-now-face-phishing-attacks-2573216-2024-07-29

[13] Onmanorama, Thrissur Rs 20 cr scam: Global IT outage uncovered Dhanya's trail of fraud, 27 July 2024, https://www.onmanorama.com/news/kerala/2024/07/27/manappuram-finance-fraud-global-it-outage-uncovered-crime-of-woman-manager.html.

[14] New Indian Express, Kerala woman employee embezzles Rs 20 cr from company to fund her online rummy addiction, arrested, 27 July 2024, https://www.newindianexpress.com/states/kerala/2024/Jul/26/kerala-woman-employee-embezzles-rs-20-cr-from-company-to-fund-her-online-rummy-addiction-arrested

[15] The New Indian Express, Be cautious of fraudulent Government e-notices: MHA issues public advisory, 14 July 2024, https://www.newindianexpress.com/nation/2024/Jul/14/be-cautious-of-fraudulent-government-e-notices-mha-issues-public-advisory.

[16] Hindustan Times, MHA issues alert on blackmail, digital arrests by cyber criminals posing as cops, 14 May 2024, https://www.hindustantimes.com/india-news/mha-issues-alert-on-blackmail-digital-arrests-by-cyber-criminals-posing-as-cops-101715702879581.html

[17] Indian Express, Panel finds cracks that help hackers target jobseekers, 28 July 2024, https://indianexpress.com/article/india/panel-finds-cracks-that-help-hackers-target-jobseekers-9479932

[18] News First, 11 Sri Lankans Deported from The UAE for Cybercrime, 7 July 2024, https://english.newsfirst.lk/2024/07/07/11-sri-lankans-deported-from-the-uae-for-cybercrime

[19] VOA, Pakistani minister confirms internet firewall, rejects censorship concerns, 26 July 2024, https://www.voanews.com/a/pakistani-minister-confirms-internet-firewall-rejects-censorship-concerns/7714552.html

[20] The Daily Star, Mobile internet, social media blocked again, 5 August 2024, https://www.thedailystar.net/news/bangladesh/news/mobile-internet-social-media-blocked-again-3669681

[21] Government of India (GoI), Ministry of External Affairs (MEA), Sixth Cyber Dialogue between India and the United Kingdom, 4 July 2024, https://www.mea.gov.in/press-releases.htm.

[22] The Hindu, Government admits BSNL data breached in May; forms telecom security panel, 25 July 2024, https://www.thehindu.com/news/national/government-admits-bsnl-data-breached-in-may-forms-telecom-security-panel/article68441779.ece

[23] The Indian Express, Cryptocurrency firm WazirX suffered a major security breach. How did it happen?, 20 July 2024, https://indianexpress.com/article/explained/explained-economics/crypto-wazirx-security-breach-cyberattack-9463004/

[24] The Economic Times, FBI pings WazirX for info on attack by 'North Korean hackers', 29 July 2024, https://economictimes.indiatimes.com/tech/technology/fbi-reaches-out-to-wazirx-over-crypto-heist-north-korean-group-lazarus-hand-suspected/articleshow/112088277.cms

[25] Business Today, Ransomware attack cripples payment systems at nearly 300 small Indian banks, 1 August 2024, https://www.businesstoday.in/technology/news/story/ransomware-attack-cripples-payment-systems-at-nearly-300-small-indian-banks-439639-2024-08-01