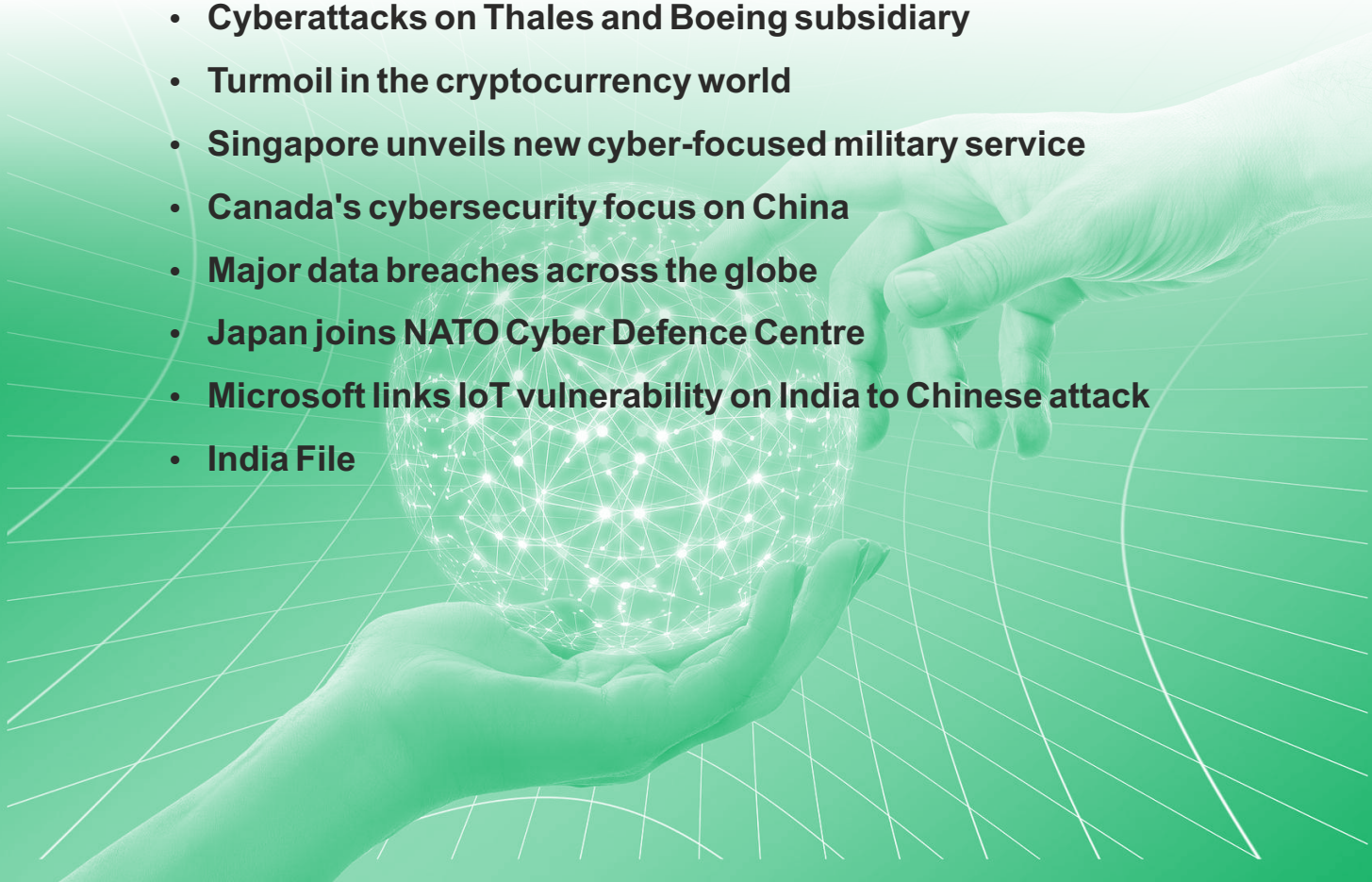
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

December 2022

- Update on Russia-Ukraine Cyber Conflict
- Country Review: Australia
- Chinese cyber offensive activities around the globe
- Cyberattacks on Thales and Boeing subsidiary
- Turmoil in the cryptocurrency world
- Singapore unveils new cyber-focused military service
- Canada's cybersecurity focus on China
- Major data breaches across the globe
- Japan joins NATO Cyber Defence Centre
- Microsoft links IoT vulnerability on India to Chinese attack
- India File



Update on Russia-Ukraine Cyber Conflict

The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2022 report finds that the war in Ukraine has shaped activity in cyberspace, though it hasn't caused the widespread devastation that was initially expected. Nonetheless, the situation has acted as a "game changer" for the global cyber domain. Following are major cyber-related activities in the month of November:

- The UK has been secretly helping Ukraine defend against Russian cyberattacks with a £6m package. The assistance focuses on forensic capabilities, hardware and other systems to bolster defences.
- Microsoft is providing Ukraine with $400 million to help with its war against Russia, extending the use of Microsoft cloud and public data centres in Europe until next year.
- Ukraine's IT army has conducted cyberattacks on 8,000 Russian resources, including defence industry and countering disinformation campaigns.
- ENISA reports that 128 government organisations in 42 countries supporting Ukraine have been targeted by state-sponsored cyberattacks, with ransomware and DDoS ranking as the top forms.
- Israel's Cyberglobes has won a contract to provide Ukraine's SBU with open source intelligence services, replacing Rayzone and Ultra.
- To safeguard its business interests, Kaspersky is stopping the operation and sale of Kaspersky Secure Connection in Russia, with the free version suspended by Nov. 15, 2022. Similarly, Yandex, a Russian search engine is hoping to transfer its most promising new technologies overseas and ditch most of its Russian business in order to avoid the effects of Western sanctions.
- In a video address to the G20, President Zelenskyy offered Ukraine's experience in resisting Russian cyberattacks during the hybrid war. He suggested creating cyber auxiliary forces and migrating to cloud services as key components of defence strategies and offered Ukraine's assistance to friendly nations. He concluded by urging close cooperation for cybersecurity.
- Western tech companies have come together to form the Cyber Defense Assistance Collaboration (CDAC) to provide direct assistance to Ukraine's cyber defence efforts. This public-private partnership for cybersecurity in wartime is worth studying for lessons that can be applied in other contexts.
- Russia based hacker group Killnet has recently launched DDOS attacks on targets related to the British Royal Family, including BACS, the London Stock Exchange, and the official website of the Prince of Wales. The group claimed the attacks were in retaliation for the UK supplying missiles to Ukraine for use against Russia.
- Russia's invasion of Ukraine has caused a ripple effect in the form of sensitive data leaks from critical infrastructure companies, including nuclear facilities in Russia, Brazil, Iran, Taiwan, Indonesia, Thailand, India, and South Africa, on the dark web.
- Retired US General Ben Hodges argues that cybersecurity is as important to

NATO logistics as missile defense, citing the example of the 2017 NotPetya attack on Ukraine which disrupted port and shipping operations.

- After Russian attacks on Ukraine's power grid, Moldova also experienced a massive blackout affecting more than 50% of the country. The attack has also caused internet outages in both Ukraine and Moldova, with emergency generators being used to restore online connectivity.

Country Reviews-Australia

- ForceNet, a service used by the Australian Department of Defence for auditable communications and personnel information sharing, has been hit by a ransomware attack, carried out by as-yet-unidentified threat actors. The attack is the latest in a string of similar attacks on Australian organisations.

- Cybercrime in Australia has seen a 13% increase to 76,000 reports in a year. The average loss for a small business is $39,000 and for a large business is $62,000. Cybersecurity threats are becoming more common and the Australian Signals Directorate's annual report warns cyberspace has become a "battleground" and "domain of warfare".

- Medibank Private Ltd, an Australian health insurer, had 9.7 million current and former customers impacted by a data breach orchestrated by hacker group in Russia called REvil, who threatened to publish the stolen data unless a ransom was paid. The hackers released the names of those who had pregnancy terminations regardless. The Australian Federal Police has identified the responsible parties.

- The Cyber Capability Fund, initially funded in the 2020-21 Budget with a three-year allocation of $30.9 million, has now been extended and will receive an additional $51 million over the course of its initial term. This fund is designed to uplift Australian law enforcement's capability to combat cybercrime.

- Australia is setting up a joint standing operation made up of 100 police and defence personnel to target ransomware groups. The operation will collect intelligence to identify ringleaders, networks and infrastructure in order to disrupt and stop their operations.

Chinese cyber offensive activities around the globe

- Researchers have discovered that Chinese-speaking threat actor APT10 has been using a sophisticated and fileless backdoor to target media, diplomatic, governmental, public sector, and think-tank targets since March. Kaspersky researchers have tracked the LodeInfo malware family since 2019, which is being used for espionage primarily against Japanese targets.

- Mark Montgomery, director of the FDD Centre on Cyber and Technology Innovation, warned Taiwan that China could use cyberattacks against them instead of military force. He said the US would research critical infrastructure to find vulnerabilities and devise ways to protect against them.

- Microsoft reported that China is using its vulnerability disclosure law to gain access to vulnerabilities before they are disclosed, potentially allowing Chinese intelligence services to develop and

deploy zero-day exploits for espionage and intellectual property theft.

- Symantec has found that a Chinese state-sponsored threat actor, known as Billbug (also known as Lotus Blossom or Thrip), compromised a digital certificate authority in an unnamed Asian country and government and defence agencies in several other Asian countries.
- Chinese police used the country's surveillance system to search for participants in protests calling for an end to Covid-curbs and criticising leaders.
- The Cyberspace Administration of China (CAC) has encouraged Huawei to make advances in core technologies to further its innovation and independence, as per the guidelines of the 20th National Congress of CPC.
- The European Commission is urging EU member countries, particularly Germany, to reduce the risks associated with Chinese telecoms equipment in 5G networks by implementing the bloc's joint 5G security guidelines.

Cyberattacks on Thales and Boeing subsidiary

Thales, a French defence and technology group, confirmed that data had been released on LockBit 3.0's public platform. The group said there has been no intrusion of its IT systems and there is currently no impact on its operations. They have identified one potential source of the data theft and are investigating the second. They are also working to minimise the potential impact. The firm has opened an internal investigation and informed the ANSSI national cyber security agency.

Jeppesen, a Boeing subsidiary, was hit by a cyberattack disrupting its services and communication channels. The company is working to restore its services as soon as possible.

Turmoil in the cryptocurrency world

- A hacker stole $28 million from cryptocurrency derivatives platform Deribit, forcing the company to halt withdrawals while they investigate the incident. Deribit is a Panama City-based exchange that allows customers to trade perpetual, futures, and options contracts. The losses will be paid through reserves, and most user funds are held in the secure "cold storage" system.
- Hackers from North Korea attempted to hack an Israeli cryptocurrency company in an attempt to allegedly fund their nuclear program. The attack was carried out by North Koreans posing as the company's Japanese supplier. Konfidas, the cyber-security company of the firm, was quick to detect the threat and managed to stop the hack.
- FTX, a bankrupt cryptocurrency exchange, is investigating a potential hack in which more than $370 million worth of crypto funds appear to be missing. A rival crypto exchange has identified the alleged hacker and promised to assist authorities in their investigation. FTX and FTX US have begun transferring all digital assets to cold storage after the bankruptcy filing.
- Moody's has reported that the cryptocurrency sector is facing growth restrictions due to its vulnerability to cyberattacks. The most recent example was FTX's hack after filing for bankruptcy. DeFi companies are particularly prone to attacks, due to their reliance on a complex chain of technologies.

- Iranian government-sponsored hackers breached a US federal government agency in February, stealing passwords and installing software to mine cryptocurrency.

Singapore unveils new cyber-focused military service

Singapore has launched its fourth military branch, the Digital and Intelligence Service (DIS), to combat modern threats in the digital domain and leverage emerging technologies. The intel directorate will support decision-making and operations through research, analysis, and integration of intelligence and operations. The combined digital and C4 unit will help the military transition into the digital age.

Canada's cybersecurity focus on China

- The Canadian Centre for Cyber Security asserts in its most recent National Cyber Threat Assessment that the state-sponsored cyber programmes of China, Russia, Iran, and North Korea pose the greatest strategic threats to Canadian online security.
- Prime Minister Trudeau has accused China of attempting to influence Canada's democracy by planting spies in MPs' offices and funding election candidates. He also noted that the federal police are investigating a secret network of Chinese "overseas police stations" in Toronto
- Canada unveiled its Indo-Pacific strategy, involving a C$2.3 billion spending plan to increase military and cybersecurity in the region. It seeks to address China's disruptive behaviour while cooperating with it on climate change and trade.

Major data breaches across the globe

- A data sample investigated by Cybernews suggests that someone is selling up-to-date mobile phone numbers of nearly 500 million WhatsApp users.
- Over 5.4 million Twitter user records were stolen using an API vulnerability and shared for free on a hacker forum, with a possibly even bigger data dump of millions of records being revealed by a security researcher.
- A Twitter data breach in 2021 was worse than initially thought, exposing nearly 5.4 million phone numbers and email addresses.
- The Irish Data Protection Commission has fined Facebook's parent company €265 million over a data breach that affected up to 525 million users.
- A ransomware attack by the Daixin Team on AirAsia may have resulted in the leak of five million customer and staff records online.

Japan joins NATO Cyber Defence Centre

Japan officially joined NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) after former Prime Minister Shinzo Abe announced the nation's intention to do so in 2018. Japan also participated in NATO's Locked Shields exercise in 2021, a large cyber war game.

Microsoft links IoT vulnerability on India to Chinese attack

Microsoft has tied an attack on seven electricity grid facilities in Northern India to a vulnerability in the Boa web server, which was discontinued in 2005 but is still widely used. The attack was part of a string of attacks on Indian critical infrastructure since 2020, and Microsoft believes that the Hive ransomware group was responsible for the most recent attack on Tata Power.

India File

- **Ransomware attack on AIIMS, New Delhi**

  A ransomware attack targeting All India Institute of Medical Sciences (AIIMS) Delhi has reportedly corrupted all files stored on the main and backup servers of the hospital, including 4 crore patient profiles with sensitive data and medical records.

- **The new Digital Personal Data Protection Bill, 2022**

  The new Digital Personal Data Protection Bill, 2022 released on November 18 is focused on personal data protection. It has hefty penalties for non-compliance and relaxed rules on cross-border data flows, but has given government agencies a blanket exemption from some requirements and diluted the remit of the Data Protection Board. MeitY officials say the new draft strikes a balance between global approaches and the Supreme Court's ruling on privacy.

- **India removes ban on VLC media player**

  India has removed its ban on VLC media player after the company went through an appeals process and addressed some of the concerns raised by the Ministry of Electronics and IT. Company president Jean-Baptiste Kempf revealed that the ban had been lifted after they met with ministry officials.

- **Defence Minister calls for joint global efforts to combat cyberattacks**

  Raksha Mantri Shri Rajnath Singh urged the international community to counter emerging security threats such as cyberattacks and information warfare during the 60th National Defence College (NDC) course convocation ceremony in New Delhi, stressing the importance of national security for the full potential of the country to be tapped.

- **India-Australia 5th bilateral cyber policy dialogue**

  The Cyber Policy Dialogue between India and Australia was held to discuss various cyber issues, such as strategic priorities, cyber threat assessment, next-generation telecommunications (including 5G technology) and capacity building for the Indo-Pacific region. The dialogue was co-chaired by the Joint Secretary (Cyber Diplomacy Division) from the Ministry of External Affairs of India and Ambassador for Cyber Affairs and Critical Technology from the Department of Foreign Affairs and Trade of Australia.

- **9th India-EU Foreign Policy and Security Consultations on cybersecurity**

  India and the European Union (EU) held the 9th India-EU Foreign Policy and Security Consultations on Tuesday. During the meeting, the two sides discussed issues such as cyber security, counter-terrorism and maritime security. The consultations were co-chaired by Sanjay Verma, Secretary (West), MEA and Enrique Mora, Deputy Secretary General for Political Affairs, European External Action Service.

- **Programme of Action to establish a permanent UN cyber forum**

  France, Egypt, and 40+ other countries proposed a Programme of Action (PoA) to end dual-track discussions - namely the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) - and establishing 'a permanent UN forum to consider the use of ICTs by States in the context of international security'. On 3 November 2022, 157 Member States, including India, voted in favour of the PoA.