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

CyberSecurity
Centre of Excellence

Major Events and Trends in Cybersecurity in 2022

AN OVERVIEW OF THE CYBERSECURITY LANDSCAPE IN 2022

Black swan events like the COVID-19 pandemic and Russia-Ukraine war have illustrated how difficult it is to predict the future, but they have also shown how vital technology is to finding solutions. The world is increasingly interconnected, bringing about new risks alongside new growth opportunities. Digital technologies, exponential growth of data, and evolving organisational needs are expanding attack threat surfaces and bringing new challenges that elevate cyber as a strategic issue. More people than ever joined the digital economy in 2022.

The year was a difficult one for cybersecurity practitioners and policy makers, with new threats arising and cybercriminals continuing to use successful techniques to accumulate significant gains. Analysts have predicted that in 2023, cross-industry collaboration will be needed to respond to new threats, data-driven intelligence will experience a surge in growth, ransomware attacks and new extortion techniques will increase.

One of the takeaways from 2022 is that cloud computing is the most reliable way to protect against cyberattacks, as demonstrated in Ukraine. Therefore, governments and other essential entities are moving more of their operations to the cloud to benefit from AI-driven security enhancements.

According to the Plato Alto Network 2022 Global Survey, in 2022, 97 percent of organisations experienced at least one breach or incident, 33 percent experienced a breached-related operational disruption. 77 percent are likely to reduce the number of cybersecurity vendors and tools they rely on, and 99 percent are looking to adopt a Zero Trust framework. Cyber insurance is becoming increasingly expensive and complex due to rising costs and compliance requirements. Insurers have had to pass their increased costs onto customers, while also requiring more stringent technical security measures before insuring them.

The past two years have seen a large number of digital supply chain breaches, where vendor-side software or hardware insecurity introduced security holes. Examples included SolarWinds and Piriform, which were attacked by booby-trapping popular products, and Kaseya, which experienced a zero day vulnerability in their VSA product that resulted in a ransomware attack. Attacks on open source repositories have seen a huge increase in the past decade, with npm and PyPI seeing a 271% and 414% increase in attacks between 2018 and 2021. This trend continued in 2022, with malicious actors submitting more than 900 malicious packages through one account in August. Platform providers are facing an overwhelming threat from these supply chain attacks. According to Deloitte 2023 Global Future of Cyber Survey, 91 percent of organisations reported at least one cyber incident or breach.

According to IBM researchers, there will be an increase in ransomware attacks, a boom in the cyber-crime-as-a-service (CaaS) ecosystem, and hackers will invent new techniques to exploit multi-factor authentication (MFA) and EDR technologies.

RUSSIA-UKRAINE CYBERWAR

The cyber conflict between Russia and Ukraine preceded the kinetic conflict by almost a month with the first major cyber attack of 2022 knocking out over 70 Ukrainian government websites, including that of the Cabinet of Ministers and the Ministries of Defence, Foreign Affairs, Education and Science on January 14. Since then, even though much of the focus has been on the kinetic conflict, the cyber conflict has also continued unabated with both sides engaged in a variety of manoeuvres, from attacks on critical infrastructure to spreading misinformation. Ukrainian cyber resilience has been enhanced through close co-operation with allies defending it against Russia. Yet another factor that has proved crucial to Ukraine's cyber resilience is the assistance provided by major software and cyber security companies. Microsoft assisted Ukraine in taking pre-emptive measures in the weeks leading up to the war with active encouragement by the US government. Microsoft also provided as much as $400 million to assist in cybersecurity efforts to Ukraine. Similarly, Amazon also contributed substantially to the Ukrainian cause.

Russia is home to a large number of hacking groups who are perceived to be sponsored by the intelligence agencies. These groups have been used to disrupt critical infrastructure, steal sensitive information, and spread disinformation. On the Ukrainian side, the government encouraged the formations of the "Ukrainian IT army", made up largely of patriotic hackers and cyber vigilante organisations from around the world. They have largely been engaged in similar activities directed against Russian entities. All these largely illegal activities can be considered a setback in the quest for setting rules of the road in cyberspace through norms of state behaviour since these activities are being both condoned and encouraged not just by Ukraine but also by Ukrainian allies such as the United States. Though on a manageable level, state-sponsored cyber attacks have been carried out also on entities in countries that support Ukraine, with the European Union Agency for Cybersecurity (ENISA) reporting 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 of attack. Similarly, after Russian attacks on Ukraine's power grid, Moldova also experienced a massive blackout affecting more than 50% of the country. The attack also caused internet outages in both Ukraine and Moldova, with emergency generators being used to restore online connectivity.

In a video address to the G20 in Indonesia, 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.

On an unrelated note, Arne Schönbohm, the chief of Germany's national cybersecurity agency, was fired following claims of suspected ties to Russian intelligence.

A consequence of the increasingly unstable cyber environment in Europe is that other countries are stepping up their cyberespionage efforts. According to Microsoft, an Austrian firm, DSIRF GesmbH, created malicious software that was detected on the computer systems of some of its clients in at least three countries. DSIRF stated that its spying tool "Subzero" was only for official use in EU states. The spyware was used to gain access to confidential information such as passwords or login credentials at an unspecified number of banks, law firms, and strategic consultancies.

CHINESE CYBER ESPIONAGE ACTIVITIES

Chinese cyber espionage by state affiliated APT groups continued unabated. Suspected Chinese hackers tampered with widely used software provided by a small Canadian customer service company, another example of a "supply chain compromise" similar to the attack vector used in the SolarWinds incident. According to PricewaterhouseCoopers, an elite Chinese hacking group with ties to operatives charged by a US grand jury in 2020 increased its activity in 2022, targeting sensitive data stored by firms and government agencies in the US and dozens of other nations. A newly detected cyberespionage group based in China was found using signed malware to attack IT service providers and telecoms companies. The operations of this advanced persistent threat (APT), known as WIP19 overlapped with Operation Shadow Force, although it is unclear whether this is a new iteration of the campaign or the work of a distinct, more sophisticated adversary employing new malware and methodologies. WIP19 primarily targeted companies in the Middle East and Asia, using stolen certificates to illegally sign many components that can be used for harmful effects. According to the Symantec Threat Hunter Team, a long-running Chinese linked cyberespionage group targeted the network of a U.S. state legislature in July, marking the group's first confirmed attack against the US government in years. Since at least 2013, the group has been known to target a wide range of companies "in support of its political and military intelligence-collection objectives." The Chinese state sponsored threat group Winnti was spotted attacking governmental entities in Sri Lanka and Hong Kong. The Winnti Group, active since at least 2007, and also known as APT41, Barium, Blackfly, Double Dragon, Wicked Panda, and Wicked Spider, is thought to be made up of many subgroups engaged in both cyberespionage and financially driven operations.

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.

Taiwan's presidential office website experienced an overseas cyberattack before Speaker Nancy Pelosi arrived in Taiwan. Private organisations including 7-Eleven, Taiwan Railway and National Taiwan University were also allegedly targeted by the Chinese. Without directly blaming any state or non-state actor, Taipei said the attacks originated from addresses in China and Russia. Taiwan's presidential office website experienced an overseas cyberattack before Speaker Nancy Pelosi arrived in Taiwan.

ATTACKS ON HEALTHCARE SECTOR

In 2022, the healthcare sector continued to face significant challenges. A report by Checkpoint Software indicated that the health care sector saw the highest increase in cyber attacks in 2022. Long-predicted staffing shortages are having an impact on healthcare service delivery all over the world, exacerbated by the burnout caused by COVID-19. Furthermore, cyber attacks are on the rise, despite the fact that, ironically, technology is frequently hailed as the solution to healthcare's problems. A cyberattack caused a "major" system outage at the UK NHS 111 non-emergency medical help line, with hosting firm, Advanced, warning that patient scheduling services could be disrupted for at least several days. The details of the cyberattack are limited, but the National Crime Agency has confirmed that it was a malicious action carried out by a threat actor.

Medibank Private Ltd, an Australian health insurer, had 9.7 million current and former customers impacted by a data breach orchestrated by a 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. A ransomware attack targeting All India Institute of Medical Sciences (AIIMS) Delhi reportedly corrupted all the files stored on the main and backup servers of the hospital, including 4 crore patient profiles with sensitive data and medical records.

CYBERCRIME ON RISE

Cybercrime flourished in 2022, particularly ransomware attacks. Data security professionals had a challenging year in 2022 due to increased data breach costs and an increase in new risks brought on by the Russia-Ukraine conflict. Unfortunately, according to current estimates in cybersecurity, the difficulty of this position will only increase in 2023. Attackers ranging from nation-states to members of the cybercriminal gig economy are likely to turn to Artificial Intelligence to sharpen the efficacy and efficiency of their attacks on critical infrastructure and supply chains, since the same techniques they have been using so far have proven to be successful.

System Intrusion was the cause of 40% of all breach events in Verizon's 2022 Data Breach Investigations Report, which was a surprise as Social Engineering and Basic Web Application Attacks had been the leading cause in the previous year.

The number of internet services assisting various cybercrimes, like business email compromise and human-operated ransomware, increased this year. Basic security measures can thwart 98% of attacks, but since cybercrime knows no borders, it's critical to cooperate to fight this threat through both public and commercial partnerships. On 21st January 2022, the Russian FSB seized 426 million rubles ($5.6 million) in a raid against 14 members of the notorious hacking group REvil, along with more than $600,000 worth of cryptocurrency and 20 luxury cars. The criminal hacking group had attacked 140 and 360 organisations in 2020 and 2021 respectively, including Brown Forman, Travelex, Grubman Shire Meiselas & Sacks, Acer, Quanta, JBS Foods, Kaseya, Sol Oriens, and Colonial Pipeline. The US government pressured Russia to take action against REvil during the 2021 Russia-United States Summit, and the G7 countries put pressure on Russia to take action against transnational criminal enterprises.

The International Committee of the Red Cross (ICRC) reported a cyberattack which compromised personal data of 515,000 people and login and password details of 2,000 staff and volunteers. The data was mainly related to missing people, unaccompanied or separated children, detainees and other people affected by conflict, disasters or migration. It is still unclear who was behind the attack.

Interpol successfully carried out Operation First Light 2022, which aimed to target telecommunications fraud, business email compromise, and money laundering. Law enforcement agencies from 76 countries raided call centres suspected of such crimes and achieved significant criminal takedowns.

MAJOR CYBER BREACHES

Uber suffered a data breach by the Lapsus$ hacking group, prompting them to shut down internal networks while investigating. The same actor is reported to have breached Rockstar Games as well. 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.

India ranked third globally and first in the Asia-Pacific region in the list of 111 countries affected by a world-wide cyberattack involving a syndicate of cybercriminals stealing passwords through a concerted phishing campaign, according to a recent report by Group-IB, a cybersecurity research firm based in Singapore. The CBI has arrested 26 cyber criminals in a coordinated effort with state police, Interpol, and agencies from other countries as part of "Operation Chakra". 87 locations were searched and 28 raided, and 11 cases have been registered against those involved in financial fraud.

Looking forward, the cybercrime-as-a-service [CaaS] ecosystem may expand in the coming year as operators introduce new tools that significantly lower the entry barrier for less experienced/technical cybercriminals. With a global recession on the horizon, hackers-for-hire may appear in search of quick and easy money.

RANSOMWARE EVERYWHERE

Ransomware is still one of the most serious threats we are facing and it appears to be increasing; in 2022, there was over a 130% rise in ransomware attacks. According to security company Sophos' 2023 Threat Report, professional ransomware operations have evolved in order to exploit industrialisation of the ransomware phenomenon. These groups specialise in gaining or purchasing access for anyone willing to pay. Organisations should expect an increase in phishing campaigns as criminals become more professionalised in their cybercrime efforts. In addition, malware strains like Emotet, Conti, and Trickbot indicated an expansion of cybercrime for hire. Ransomware-as-a-service is enabling criminals without deep technical skills to make money, either by extorting a ransom for decryption keys or selling stolen data on the dark web or to a victim's competitors. Accordingly, organisations should also expect an increase in email phishing attacks. Vital defence strategies include timely patching and updating of software.

Oil India's operations in Assam were disrupted by a cyberattack on April 10 and the company received a ransom demand of USD 75,00,000 (about Rs 57 crore). A case was registered under various sections of the Indian Penal Code and the Information Technology Act, 2000.

A new analysis by cybersecurity firm Trellix found that cyber-attacks on critical infrastructure have increased significantly, with India seeing a 70% increase in ransomware activity in Q4 2021. Russian and Chinese backed groups were responsible for over half of the incidents, and malware was the most used technique. Individuals were the primary target, with healthcare, transportation, shipping, manufacturing, and IT industries also seeing a sharp increase in threats.

Costa Rica was hit with Conti ransomware attacks, prompting the newly elected president to declare a national emergency. The attack resulted in 672 GB of data being leaked from Costa Rican government agencies, including the Ministry of Finance, Ministry of Labor and Social Security, Social Development and Family Allowances Fund, and Interuniversity Headquarters of Alajuela. CISA has announced the formation of a joint ransomware task force as part of CIRCIA, an omnibus spending bill passed in March. The task force will require critical infrastructure organisations to report significant cybersecurity incidents or ransom payments within 72 and 24 hours, respectively, to the federal government.

TAMING CRYPTOCURRENCIES

Moody's 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. Decentralized finance (DeFi) companies are particularly prone to attacks, due to their reliance on a complex chain of technologies. Ronin Network, a gaming-focused blockchain network, was hacked and coins worth over $600 million were stolen, making it the second-largest cryptocurrency hack ever. The hack is even bigger than the Mt. Gox hack of seven years ago, which led to increased regulation in space. Last year saw a 79% increase in cryptocurrency-based crime as adoption of crypto has grown. North Korean state-sponsored threat actors have laundered $100 million from the Harmony's Horizon blockchain bridge, and US authorities seized $500,000 worth of Bitcoin from North Korean hackers. In 2021, the hackers used ransomware to target healthcare providers, extorting money from organisations and returning ransom payments to two hospital groups. In total, North Korean hacking groups have made over $1 billion for their government.

A security flaw cost Nomad, a bridge protocol for transferring crypto tokens across different blockchains, nearly $200 million. Blockchain data showed that various accounts drained the software system of funds over hours and in small batches. Thousands of crypto wallets linked to the Solana ecosystem were emptied ($ 4 million in total) by hackers who stole both Solana (SOL) and USD Coin using the owners' private keys (USDC). Solana linked the attack to Slope mobile wallet app accounts. Russian national Alexander Vinnik, the alleged operator of the illegal cryptocurrency exchange BTC-e, was extradited from Greece to the United States will face charges in the Northern District of California. BTC-e facilitated transactions for cybercriminals all over the world and received more than $4 billion in bitcoin during its operation.

The United States sanctioned virtual currency mixer Tornado Cash and Blender.io, a North Korea-linked crypto mixing service, accusing them of helping hackers, including Lazarus Group from North Korea, in laundering proceeds from cybercrime. Tornado Cash, one of the largest mixers identified by the Treasury as problematic, has reportedly laundered more than $7 billion in virtual currency since its inception in 2019. Crypto bridges, which connect blockchain networks, have become major targets for cybercriminals. According to research from blockchain analytics company Chainalysis, breaches on cross-chain bridges have cost users a total of almost $1.4 billion this year. The largest incident involved the theft of a record

$615 million from Ronin, a bridge that supported the well known non fungible token game Axie Infinity.

India's Enforcement Directorate has frozen assets worth $46.4 million from Flipvolt Technologies, the local entity of crypto exchange Vauld, after it failed to provide a complete trail of crypto transactions and KYC details for wallets linked to predatory lending firms. 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. Iranian government-sponsored hackers breached a US federal government agency in February, stealing passwords and installing software to mine cryptocurrency.

EMERGING TECHNOLOGIES AND CYBERSPACE

According to Deloitte 2023 Global Future of Cyber Survey, cloud, data analytics, Operational Technology/Industrial Control Systems, Artificial Intelligence/ Cognitive Computing, and 5G are emerging technologies that will affect cyberspace. Malicious hackers have a lot of present-day and future opportunities because of the metaverse. They might develop a virtual deepfake of online avatar that can move and behave like an individual in five to 10 years. But that doesn't imply attacks on the metaverse aren't already happening right now. The first metaverse attack that has an impact on business will come from a well-known threat vector that has been updated for the VR era.

By utilising security intelligence based on data, insights can be gained into how to make the cloud ecosystem security even stronger, including multi-cloud infrastructures and cloud applications. Microsoft reported in 2022 that they tracked over 250 different cyber actors, monitored 35 ransomware groups, and processed 43 trillion security signals each day, including 1,200 password attacks per second. The strength of AI and threat intelligence can be innovatively combined on the defence side as well, enabling threat intelligence to be utilised broadly to identify and interrupt the spread of an assault, if not completely prevent it. To further shared knowledge, the security community will also witness stronger collaborations and intelligence sharing. Organisations must have a comprehensive understanding of their digital estate, which includes data, infrastructure, identity, and applications for IT, OT, and IoT, from clients to the cloud. It is crucial that they approach their infrastructure from the outside in order to determine what is vulnerable to attackers and how to secure those assets.

Huawei has been involved in a number of projects in island nations, such as Mauritius, Comoros, Madagascar and the Solomon Islands. The company is supplying infrastructure for Smart City projects and mobile communication towers, and is involved in submarine cable system installations. 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.

INDIA'S CYBER GOVERNANCE

The NCRB reported that cybercrime in India increased by 11% in 2020, with 50,035 cases reported. Fraud accounted for 60.2 percent of all cyber-crime cases, while sexual exploitation and extortion accounted for 6.6 percent and 4.9 percent respectively. Some states such as Punjab and Rajasthan do not have a single cybercrime unit, while Andhra Pradesh, Karnataka and Uttar Pradesh only have one or two. Mumbai Police have set up 6 cybercrime investigation and forensic labs to tackle the growing number of cybercrime cases, while Delhi and Chandigarh are also setting up their own cyber police stations and directorates. The Central government has taken several initiatives to help State Governments build their LEA capacity to combat cybercrime, including establishing the National Cyber Forensic Laboratory in New Delhi, launching the National Cyber Crime Reporting Portal, launching the Citizen Financial Cyber Fraud Reporting and Management System, and creating seven Joint Cyber Coordination Teams covering the whole country. MEITY Minister Rajeev Chandrasekhar announced that the Indian government has allocated over Rs 1,300 crore for online safety, trust, and accountability programs from 2019-20 to 2022-23.

The Ministry of Electronics and Information Technology blocked 54 apps, This follows the 2020 and 2021 bans of over 200 and 59 Chinese mobile applications respectively.

India is establishing a CSIRT housed under its Central Electricity Authority to protect its power grids from cyberattacks. The team will be composed of professionals recruited through the Combined Engineering Services Examination. Jitendra Singh, the Union Minister of State (Independent Charge) of the Ministry of Science and Technology and Earth Sciences, told the Lok Sabha that 660 innovations have been developed under the National Mission on Interdisciplinary Cyber-Physical Systems, compared to a target of 6,824. Additionally, out of the mission target of 30,694 Human Resource Development, 3,145 have been achieved.

The Indian Ministry of Electronics and Information Technology issued a direction that requires service providers, intermediaries, data centres, body corporates, and government organisations to notify any cyber incidents within 6 hours of detection. This would have implications on how these entities collect and store data, as well as the need to share it with the government in case of a breach. Companies offering virtual private network (VPN) or cloud services may be required to maintain customer data for five years. Failing to comply with the directions may result in punitive action.

MeitY issued a new set of IT Rules 2021 amendments These amendments require intermediaries to respect users' constitutional rights, and create an appellate body 'Grievance Appellate Committee' for users to appeal against the grievance redressal processes of intermediaries. CERT-In gave MSMEs, Data Centres, VPS providers, Cloud Service providers, and VPN Service providers an extension until September 25, 2022 for implementing new cyber security rules. These rules require data centres, VPS and cloud service providers to keep a five-year record of customers' personal information.

India has changed its telecom licensing rules to make it more difficult for Chinese vendors to sell to local operators. The DoT has updated the procurement rules to ensure cybersecurity and 5G services will be operational before the end of 2022. Minister of Home Affairs Amit Shah announced the formation of a committee, led by the Union home secretary, to develop a unified strategy to combat cyberattacks in order to protect national security. The committee will include representatives from all state governments and departments. The Ministry of Home Affairs (MHA) launched an on-the-ground investigation, beginning in Jamtara, India's "phishing capital," to develop a roadmap for combating cybercrime. Senior ministry officials visited cities notorious for cyber crooks — Jamtara, Deoghar, Giridih, and Bokaro — and met with state officials.

The Unique Identification Authority of India (UIDAI) established a bug bounty programme with the aim of enhancing security around the Central Identities Data Repository (CIDR), the database that houses the biometric data of over 1.3 billion holders of Aadhaar cards. Indian Computer Emergency Response Team (CERT-In) in collaboration with Power-CSIRTs (Computer Security Incident Response Teams in Power sector), successfully designed & conducted the Cyber Security Exercise "PowerEX" for 193 invited Power Sector Utilities. The Exercise Planner Team of Power-CSIRTs' officials worked along with the CERT-In team on the exercise day as Exercise Coordinators. The objective of the exercise was to "Recognize, Analyse & Respond to Cyber Incidents in IT & OT Systems".

The Department of Telecom made available for public comment the draft Indian Telecommunication Bill, 2022, which aims to reform existing telecom laws and regulations and make them "future ready." 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 removed its ban on VLC media players 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. 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.

The National Security Council Secretariat organised the National Cyber Security Incident Response Exercise (NCX India) from 18-29 April, with National Security Advisor Ajit Doval inaugurating it. Cybexer Technologies, an Estonian cybersecurity company, provided training for more than 140 participants, who were taught various key cyber security areas such as Intrusion Detection Techniques, Malware Information Sharing Platform (MISP), Vulnerability Handling & Penetration Testing, Network Protocols & Data Flows, and Digital Forensics.

INDIA'S CYBER DIPLOMACY

Indian cyber diplomacy had a full calendar through the year. It began with the Senior Officers Meeting of the India-US Homeland Security Dialogue was which held on Jan 12th 2022 and discussed various security issues, such as counter-terrorism, cyber security, critical infrastructure and global supply chains, maritime security, aviation security, customs enforcement, and trade security. The dialogue was reestablished after discussions between

India's Ambassador to the US, Taranjit Singh Sandhu, and DHS Secretary Alejandro N. Mayorkas.

The first Colombo Security Conclave Virtual Workshop was held from 10th to 11th January 2022, with delegates from Sri Lanka, Maldives, India, Mauritius, Seychelles, and Bangladesh. It addressed key areas such as Deep Web and Dark Net Investigation and Challenges, Digital Forensics, Cyber Threat intelligence, and Defensive Operations in Cyber Domain. It follows the 5th Deputy NSA Level Meeting of the Colombo Security Conclave held on 4th August 2021 which agreed on four pillars of cooperation including Maritime Safety and Security, Terrorism and Radicalization, Trafficking and Organized Crime and Cyber Security and Protection of Critical Infrastructure.

The 2nd ASEAN Digital Ministers' Meeting approved the India-ASEAN Digital Work Plan 2022, which includes combating the use of stolen and counterfeit mobile handsets, WiFi access network interface for public internet, and capacity building in ICT such as IoT, 5G and advanced satellite communication.

Dr. S. Jaishankar, Minister of External Affairs co-chaired the 12th Foreign Ministers' Framework Dialogue (FMFD) and the 1st Foreign Ministers Cyber Framework Dialogue, with Australian Foreign Minister Ms. Marise Payne, in Melbourne, Australia on 12 February 2022. The Ministers discussed the progress made towards implementation of the India Australia Framework Arrangement on Cyber and Cyber-Enabled Critical Technology Cooperation and the subsidiary Plan of Action which was signed in June 2020 on the side-lines of the Virtual Leaders' Summit held between Prime Minister Shri Narendra Modi and Australian Prime Minister Scott Morrison. 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.

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.

India and the UK held their Annual Cyber Dialogue in London on 11-12 April 2022. The Indian delegation was led by Ms. Muanpuii Saiawi, Joint Secretary Cyber Diplomacy Division, MEA. The UK delegation was led by Mr. Will Middleton (Cyber Director, Foreign, Commonwealth and Development Office). The meeting was attended by senior officials from several government ministries. Both sides welcomed the substantial bilateral engagement which covered cyber governance, deterrence and mutual resilience. They reiterated their commitment to a joint programme of action and next steps in implementing the Enhanced Cyber Security Partnership agreed upon by the two Prime Ministers in May 2021.

India and Thailand agreed to strengthen defence and security cooperation, including cybersecurity. Dr S Jaishankar and his Thai counterpart Don Pramudwinai, stated to the media that they had agreed to strengthen cooperation in defence and security, including cyber-security and the exchange of personnel and expertise. According to Dr S Jaishankar, the decision was made to increase joint training and exercises in defence and security, as well as recognise the importance of further cooperation in ICT.

The Deputy NSA, NSCS- led Fourth India-US Bilateral Cyber Dialogue was held in Washington DC, USA from 21- 23 September 2022. India also participated in the U.S. led Counter Ransomware Initiative [CRI] meeting held in Washington D.C. on November 1, 2022.

A number of UN fora held meetings over the year with active participation by India. The *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes met in New York from 28 February 2022 to 11 March 2022. Mr. Eric Do Val Lacerda Sogocio from Brazil was elected as Vice Chair, and the Japanese candidate was elected with consensus from the Asia Pacific region.

The Second Substantive Session of the Open Ended Working Group on security of and in the use of information and communications technologies 2021-2025 was held at New York from 28 March 2022 to 1 April 2022. Resolution 73/27 established the Open-Ended Working Group (OEWG), which all UN Member States are invited to participate in. The OEWG process also provides the possibility of holding inter-sessional consultative meetings with industry, non-governmental organisations and academia.

The Third Substantive Session of the new Open Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025 was held in New York from 25 to 29 July 2022. The Third Substantive Session of the OEWG adopted its First 'Annual Progress Report' on consensus basis. This marks an important milestone in the work of the OEWG to further discuss the six pillars of its mandate and build common understanding and consensus on the ICT security matters under the UN framework. India reiterated its call for creating a "permanent mechanism for exchanging views and ideas related to capacity-building in ICTs" in the form of an integrated and comprehensive portal.

The First Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in New York from 28 February 2022 to 11 March 2022 in Hybrid mode. The Second Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in Vienna from 30th May 2022 to 10 June 2022 on Hybrid mode. The Third Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in New York from 29 August 2022 to 09 September 2022 in Hybrid mode.

The 9th ARF Open Ended Study Group (OESG) on Confidence Building Measures to reduce the risk of conflict stemming from the use of ICTs was held on 10.5.2022 and 4th ARF Inter Sessional Meeting on Security of and in the use of ICTs was held on 13.5.2022 on virtual mode. India actively participated in both the meetings. Shri Saurabh Kumar, Secretary (East), virtually attended the ASEAN Regional Forum Senior Officials' Meeting (ARF SOM) on June 9, 2022. He also shared India's perspectives on the threat posed by terrorism and the challenges of cybersecurity. The meeting reviewed the 27-member ARF's activities and exchanges over the previous year and deliberated on its future plans and activities. Senior officials discussed regional and international developments, as well as the Covid-19 pandemic, terrorism, maritime security, and cybersecurity.

INTERNATIONAL DEVELOPMENTS

Japan has formed a new cyber-defense organisation to improve its response to cyber-attacks. Australia also recently opened a new cyber and foreign intelligence centre in Canberra to boost its capabilities, with the aim of identifying threats and disrupting potential adversaries. The US State Department has set up a Bureau of Cyberspace and Digital Policy to tackle international cyberattacks and criminal ransomware, with three policy units focusing on international cyberspace security, information and communications policy, and digital freedom. It is also working to create an Office of Special Envoy for Critical and Emerging Technology.

NATO's Locked Shields cyber exercise was held with simulated attacks on power grids and financial-messaging systems. Participants from NATO countries as well as allies including South Korea, Brazil, Finland, and Sweden took part in the simulations, which included a power grid for the first time. The Financial Services Information Sharing and Analysis Center, an industry group, and some top global firms helped plan the financial part of the exercises. Experts had to defend against mock cyberattacks while also being drilled on legal disputes and media notifications. South Korea's military participated in a multinational cyber exercise led by the U.S., with 25 countries and 18 personnel. The Cyber Flag exercise included seminars and field training to increase readiness against malicious cyber activities.

Slovenian Nuclear Safety Administration conducted a Cyber Security Exercise to Test Nuclear Security Capabilities, involving key Slovenian nuclear sector stakeholders. The exercise featured real operational technology systems with insider threats, external cyberattacks, and physical intrusions into a fake nuclear facility, demonstrating the consequences of a computer security compromise of critical operational control. A new law in Canada requires companies operating in critical infrastructure sectors to report cyberattacks to the government and strengthen their cyber security systems. The law applies to federally regulated firms, but the government hopes that provinces and territories will also pass similar legislation to improve the cybersecurity of entities under their jurisdiction. Records must be kept of cyber security programmes, incidents, risk mitigation and government-ordered actions.

The AUKUS Joint Steering Groups, consisting of representatives from Australia, the United Kingdom, and the United States of America, held meetings on July 28 and 29 to examine progress on key defence capabilities. They decided to focus on near-term capabilities in cyber, counter-hypersonics, and hypersonics, as well as joint military capabilities.

In June, Israel and Iran were engaged in cyber-attack allegations. Microsoft disrupted a campaign against Israeli organisations conducted by the Lebanese group Polonium, linked to Iran's Ministry of Intelligence and Security. The hacktivist group Gonjeshke Darande also targeted Khouzestan Steel Company, one of Iran's largest steel manufacturers.

Mandiant identified a ransomware family and Telegram persona targeting the Albanian government, indicating a willingness to take risks against countries perceived to be working against Iranian interests. Albania cut diplomatic ties with Iran and expelled its diplomats after a cyberattack, which was supported by the US and promised a response to protect its NATO ally. In addition, Albania has also been subjected to more cyberattacks from Iran, prompting the US Treasury Department to impose sanctions on Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence. CISA and the FBI have issued a joint warning with suggested safeguards in case the campaign spreads elsewhere, while Israel has offered cyber defence assistance to Albania.

Albania and Iran have had tense relations since 2014, when Albania accepted 3,000 members of the exiled opposition group People's Mujahideen Organization of Iran, also known as Mujahideen-e-Khalq in Farsi, who have settled in a camp near the country's main port of Durres. Furthermore, Albania reported that it has been subjected to additional cyberattacks from Iran, presumably in response to Tirana's split with Tehran over the July cyber incidents. Iran allegedly took down the Total Information Management System (TIMS) used in Albania for border control. As the contours of Iranian cyberattacks on Albania's government networks became clearer, the US Treasury Department imposed sanctions on Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence, Esmail Khatib, for their role in the NATO country's cyberattacks. However, Iran condemned the US action, with the Foreign Ministry claiming that the Albanian government made a false accusation. The US Cybersecurity and Infrastructure Security Agency (CISA) has issued a joint warning with the FBI outlining Iran's cyber campaign against Albania. The warning includes suggested safeguards and mitigations in the event that the campaign spreads to targets outside of Albania. Due to shared experiences of being targeted by Iranian cyber operations, Israel has also offered cyber defence assistance to Albania.

The US National Defense Strategy, released in October 2022, emphasises deterrence through resilience and cost imposition, such as offensive cyber operations, to counter the threat posed by four adversaries- China, Russia, North Korea, and Iran- with strong cyber capabilities. Zero-trust principles and encryption are recommended for resilience.

Singapore has launched the Digital and Intelligence Service (DIS) as its fourth military branch, to address modern threats in the digital domain and leverage emerging technologies. The unit will provide research, analysis and integration of intelligence and operations to support decision-making and operations. 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.

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. The National Intelligence Service (NIS) of South Korea has been accepted as a contributing participant for the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the first in Asia. South Korea's admission to the group comes against the backdrop of Russia's invasion of Ukraine, indicating a hardening of commitment among US allies in reaction to Russian and Chinese threats. However, it is unclear whether the events in Ukraine influenced NATO's decision to approve South Korea's membership. The NIS applied to join the organisation in 2019 and has since taken part in two Locked Shields exercises, the world's largest international live-fire cyberdefense exercise. The CCDCOE now includes 27 NATO member countries as well as five non-NATO contributing participants, the others being Austria, Finland, Sweden, and Switzerland.

The US Cyber Command's Cyber National Mission Force (CNMF) deployed a hunt forward team to undertake defensive cyber operations alongside partner cyber forces at the invitation of the Lithuanian government. Along with its allies, the US cyber operators searched for harmful cyber activity on important Lithuanian national defence systems and Ministry of

Foreign Affairs networks. This was the first shared defensive cyber operation between Lithuanian cyber forces and CNMF in that country

Researchers have revealed findings about POLONIUM, an Iranian-affiliated APT group based in Lebanon. Since September 2021, the group has targeted more than a dozen organisations in Israel, with their most recent actions observed in September 2022. Targeted verticals include engineering, IT, law, communications, branding and marketing, media, insurance, and social services.

Critical Infrastructure

JNPCT, India's busiest state-owned container port, was crippled in Feb 21 due to a suspected cyber-attack on its management information system (MIS). This led to the diversion of one vessel and JNPCT not accepting vessels until the system was restored.

In the United States, President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law on March 15, 2022. After failing to pass similar legislation in recent years, the House and Senate unanimously approved the bipartisan bill on Mar 9 and 11 respectively, due to cyberattacks on critical infrastructure providers and increasing concerns over Russian and Ukrainian conflict. The legislation requires hospitals, power plants, water utilities, airports, and other key infrastructure to notify the Department of Homeland Security within 72 hours of a cyberattack. The FBI and Justice Department sought modifications to assure that they were informed of the attacks and for such information to be kept out of the Freedom of Information Act.

Recorded Future, a US-based cyber security firm, reported that Chinese government-linked cyber groups targeted 7 Indian State Load Dispatch Centers in northern India in a large cyber-espionage campaign. Union Power Minister R K Singh also noted that China has attempted 3 "probing cyberattacks" on India's power infrastructure in Ladakh since December 2021, but these have been unsuccessful due to prevention measures. Chinese government-backed hackers reportedly targeted India's National Informatics Centre (NIC) in a cyberattack, with RedAlpha spoofing login pages for the NIC, which manages India's government IT infrastructure and services.

Tata Power Company Limited was hit by a cyberattack, causing some of its IT systems to be impacted. The company has taken steps to retrieve and restore the systems and the Maharashtra Police's cyber wing received an intelligence input about a threat to Tata Power and other electricity companies. Black Reward, a group claiming to support Iran's anti-government protests, hacked the Atomic Energy Organization of Iran (AEOI) and published emails from its Nuclear Energy Production and Development Co. subsidiary online without authorization. Microsoft has linked an attack on seven electricity grid facilities in Northern India to a vulnerability in the Boa web server, which was discontinued in 2005. The attack is believed to be part of a string of attacks on Indian critical infrastructure since 2020, and it is suspected that the Hive ransomware group was behind the most recent attack on Tata Power.

Australia passed amendments to the Security of Critical Infrastructure Act 2018 on December 2, 2021, to deliver an enhanced framework for the security of critical infrastructure. The amendments expanded the list of critical sectors from four to eleven. Critical infrastructure is now deemed to consist of entities in communications, financial services and markets, data storage or processing, defence industry, higher education and research, energy, food and grocery, health care and medical, space technology, transport, and water and sewerage.

The government also arrogated to itself the power to intervene and “take over” entities in the event of cyber incidents as a “last resort.” This power has been criticised by cybersecurity companies for setting a “troublesome global precedent” since they were not “subject to reasonable due process, which would normally allow affected entities to appeal or have these decisions independently reviewed.” The requirement of reporting cyber incidents within a 12 hour framework would also result in companies having to set aside manpower to fulfil such duties at a time when they would be better engaged in responding to such incidents

For its part, the government has maintained that these powers would be used only in the rarest of circumstances and invoking them required a process in which the Minister for Home Affairs has to get agreement from the Prime Minister and the Minister of Defence.

Political Espionage

Amidst the Russian-Ukrainian conflict, many state-backed threat actors were scaling up their operations. Microsoft's intelligence report revealed Russian efforts, including espionage activities against Ukraine and its allies.

The Belgian Foreign Ministry urged the Chinese government to take action against malicious actors that had attacked the servers of the Ministry of Defence and other agencies.

APT 28, believed to be of Russian origin targeted Ukrainian Organizations with email purporting to come from Computer Emergency Response Team of Ukraine (CERT-UA). The email contained malware designed to steal data. APT 28 also targeted Ukrainian media organizations, government institutions, and foreign policy think tanks in the United States and the European Union. According to Microsoft, it took control of the internet domains used in the attack and redirected the site traffic to a sinkhole.

Chinese APT actor Scarab also used a similar playbook in Ukraine, sending out malware in mails mimicking the National Police of Ukraine. Ukraine was also used as clickbait against European diplomatic organisations by the Chinese APT actor Bronze President with fake emails with file names such as 'Situation at the EU borders with Ukraine.zip'. Mustang panda had previously focused and South and South East Asia, targeting telecom firms in India, Myanmar, Tibet and Taiwan

Palestinian actors used Facebook profiles as bait on Israeli military, law enforcement and emergency services employees. Iranian hackers reportedly targeted Jordan’s Foreign Ministry as part of a phishing campaign. The attack was attributed to a threat group APT34, believed to be running operations from Iran. The malicious mail was sent via a Microsoft Outlook account using Microsoft Excel as an attack vector. According to Checkpoint, Iranian spear-phishing operations were also used against former Israeli and US high-ranking officials. The list of targets also included research fellows in think-tanks and other research institutions.

The CISCO Thalos Intelligence Blog revealed that a Pakistani APT had been targeting Indian government officials using the CrimsonRAT trojan implanted on fake sites mimicking legitimate military and defense organizations. The downloader executables included fake versions of the Kavach authentication app.

INDUSTRIAL ESPIONAGE

China based threat actors targeted major telecom and network service providers in the United States, scanning for routers with known vulnerabilities. The Russian GRU-backed APT group, Sandworm, famous for attacking infrastructure in Ukraine targeted Asus routers in many countries including the US, Canada, Italy and Russia using the Cyclops Blink malware. It is believed this was for the purpose of using them as C&C servers for botnet attacks. The FBI removed the malware and disrupted the botnet through a court-authorised operation.

Chinese state-sponsored hackers carried out a series of attacks on Indian power grids in the border areas in North India according to Re3cordeed Future. The specific targets were state load dispatch centres and the attacks were repelled successfully according to the Power Minister.

In a campaign running form April to Jun 2022, malicious actors targeted Australian, Canadian, German, Japanese Swedish , and Taiwanese wind farming companies operating in the South China Sea. The companies were compromised through phishing attacks and information related to their activities in the contested South China sea area were exfiltrated.

India-based enterprise software firm Zoho had a vulnerability in its software exploited by Chinese hackers to infiltrate organisations in critical sectors such as defence, energy, healthcare, education and technology.

The China-nexus adversaries were reported to have significantly increased operational scale in 2022. According to the Crowd Strike 2023 Global Threat Report, technology-related entities were repeatedly at the receiving end of China-linked economic espionage campaigns targeting R&D data, proprietary information, and trade secrets. These threat actors overwhelmingly targeted Taiwan-based technology organizations in 2022. To counter the increasing threat, Taiwan's government proposed a new law setting out rigorous punishment for economic espionage.

Chinese hacker group APT27, reportedly targeted several German companies in sectors such as pharmaceuticals and technology to steal trade secrets and intellectual property.

In January 2022, Federal Bureau of Investigation (FBI) Director Christopher Wray shared concerns over China's economic-espionage campaigns flagging such operations as a threat to innovation and economic security of the US and its allies. In July, Christopher Wray and Ken McCallum, the Director General of MI5, delivered a joint address raising alarms about the Chinese government as the most significant long-term threat to economic security.

Cyber reason, a cybersecurity technology company, uncovered a massive Chinese-backed industrial espionage ring targeting technology and manufacturing in the US, Europe, and Asia and stealing sensitive proprietary information. The group behind the espionage operations, Winnti (tracked as APT41, Blackfly, and Barium in cybersecurity circles), is believed to have been active since 2010.

In November 2022, the Chinese government intelligence officer was sentenced to 20 years in prison by the federal court in Cincinnati for economic espionage and attempting to steal trade secrets. The convicted used several means to exfiltrate trade secrets from US-based firms, including malware installation in systems.

North Korea-based threat actor Lazarus Group was reported to have exploited Log4j vulnerabilities in VMware Horizon to steal trade secrets and siphon off proprietary intellectual property. The same group was also behind phishing campaigns against aerospace and defence contractors in early 2022.

The Cybersecurity and Infrastructure Agency (CISA), National Security Agency (NSA), and FBI issued an alert elaborating on Russian-backed actors targeting cleared defence contractors (CDC) to acquire sensitive unclassified information on weapons and aircraft designs.

Amidst the ongoing Russia-Ukraine conflict, many Western companies reportedly raised the alarm over President Putin's pronouncements on the role of Russia's Foreign Intelligence Services in fostering technological advancements in the country. The pronouncement was made in the context of mounting pressure on Russia's economy, severely impacting its technological advances. The statement is broadly interpreted as Russia's readiness to use industrial espionage for economic benefits.

MAJOR CYBER INCIDENTS IN THE SOUTH ASIAN REGION

Meta, Facebook's parent company, reported that it took action earlier this year against two cross-platform cyberespionage operations that used various online services to distribute malware in South Asia. Bitter APT (T-APT17) is the first group of hackers that Meta disrupted during the second quarter. The group has been active since at least 2013, targeting entities in the energy, engineering, and government sectors in India, New Zealand, Pakistan, and the United Kingdom. The second group of hackers APT36 is based in Pakistan. The group is believed to be connected to the Pakistani government. APT36 has been observed targeting government officials, human rights activists, military personnel, students, and non-profit organisations in Afghanistan, India, Saudi Arabia, and the United Arab Emirates.

INDIA

- Two Indian companies faced major cyberattacks in the month of May. According to a police complaint filed by the payment gateway company, Razorpay, hackers and fraudulent clients stole 7.3 crore by interfering with and manipulating the authorisation process of Razorpay Software to authenticate 831 unsuccessful transactions. Additionally, hundreds of passengers were stuck at airports and on planes following a recent attempted ransomware attack on SpiceJet, a domestic airline. After aeroplane departures slowed, aviation operations were disrupted for almost four hours.
- Malaysia Dragon Force, a Malaysian hacktivist group, called upon hackers all over the world to launch cyberattacks against the Indian government's information technology (IT) infrastructure. The group announced its plans on Twitter, calling the move a "special operation." Dragon Force has posted multiple instances of what they claim are breaches of various websites and departments in India since its announcement. The collective claims to have taken down the services of Hostnet India, a popular web hosting company in India, resulting in the shutdown of multiple companies' websites. Dragon Force also claimed to have published a list on Twitter that contained information belonging to members of the Indian government. However, the email

addresses listed in the alleged database appeared to be personal addresses rather than official ones.

- Akasa Air admitted to a data breach that allowed unauthorised individuals to view data from some of its customers. The incident was "self-reported" to CERT-In by Akasa Air. According to cyber security firm CyberX9, Vi (formerly Vodafone Idea) has exposed its users' data, which includes the records of more than 20 million postpaid customers, to possible breach. Phone numbers, addresses, call logs, SMS records, and mobile Internet usage information for approximately 301 million customers, including all postpaid users, were discovered to have been leaked online. Vodafone Idea denied the data breach, calling the report false and malicious. Hackers were discovered to have leaked Provident Fund (PF) data for approximately 28 crore Indians. A cybersecurity researcher from Ukraine discovered that details such as Universal Account Numbers (UANs), names, marital status, Aadhaar details, gender, and bank account details were exposed online.

- According to Uttar Pradesh's cybercrime unit, Chinese scammers stole $529 million from Indian residents using instant lending apps, part-time job offers, and bogus cryptocurrency trading schemes. The scammers advertised their scheme via bulk TXT messages, which the police traced to the Middle Kingdom, with some operators based in Nepal and directed by Chinese threat actors. Fake websites and cryptocurrency apps were set up to entice investors. Furthermore, so far, the Enforcement Directorate has conducted search operations on the 12 Chinese companies involved in the Part-Time Job Fraud case in Bengaluru, seizing Rs.5.85 crore under the Prevention of Money Laundering Act, 2002.

PAKISTAN

- Pakistan released its first ever National Security Policy on 14th January 2022. The policy aims to focus on a non-traditional security approach that focuses on a citizen centric framework instead of a one dimensional security policy based on the development of military capabilities. In terms of Pakistan’s strategy on cyber, the report contains three related sections, namely: 1) Information and Cyber Security Threats, 2) Hybrid Warfare, 3) Space, Information and Security. The document considers the cyber and space domains along with land, air, and sea important for territorial integrity which can be achieved by ‘defence, deterrence, astute diplomacy, and the building of robust space and cyber capabilities’. In terms of maritime security, Pakistan is worried about ‘cyber intrusion and surveillance of sea lines of communication along the Indian Ocean’. The 'Information and Cyber Security Threats' section discusses the importance of instituting robust mechanisms to protect cyberspace, investments in cyber security of critical infrastructure, and building domestic capacity to monitor and minimise both surveillance and cyber intrusion. In the ‘Hybrid Warfare’ section, the policy states that hybrid warfare tools include ‘information and cyber warfare, disinformation, influence operations, lawfare, and economic coercion’ and to counter these threats, Pakistan will adopt a ‘holistic, interconnected whole-of-nation’ approach. In the ‘Space, Information and Cyber Security’ section, the emphasis is on ‘combating disinformation and influence operations while enhancing information and cyber security, data security, and surveillance capacity'.3 Overall, the flaws in the cyber section of the strategy are similar to those that have bedeviled cybersecurity strategies of other countries; too much vagueness, lack of a robust timeline for implementation, and difficulty in formulating the core cyber issues for the country

BANGLADESH

- Bangladesh is preparing to implement a cybersecurity plan aimed at ensuring the proper functioning of cyberspace by increasing resilience to the growing threat of cyberattacks. The Digital Security Agency under the Information and Communication Technology (ICT) Division has already drafted the Bangladesh Cybersecurity Strategy for 2021-2025. The ICT Division will place the strategy before the cabinet for approval soon, after making necessary changes, if any, to it based on recommendations from other stakeholders. The proposed cybersecurity policy, which is the first of its kind in Bangladesh, specifies that all ministries will be equipped with particular software and qualified staff to safeguard themselves against cyberattacks. According to ICT Division officials, the draft strategy focuses on 10 points to confront future cyber challenges and improve the country's capacity in cyberspace. The major targets set in the draft document include enhancing national cybersecurity governance and ecosystem, improving organisational management and business operation, strengthening cybersecurity incident management and active cyber defence, enhancing national cybersecurity capacity, nourishing cybersecurity knowledge through education, and promoting a competitive local industry and ecology.17
- The UN Development Programme (UNDP) and the government of Bangladesh's ICT Division have signed an agreement to launch a Cyber Security campaign for youth and children in select Least Developed Countries (LDC) countries. The ICT Division will provide USD 5 million to implement the Cyber Security campaign over 5 years. Money was raised from the 'Golden Jubilee Bangladesh Concert' that took place on May 6 at the Madison Square Garden in New York. Under this partnership, UNDP Bangladesh Bangabandhu Sheikh Mujibur Rahman International Award on Cyber Security Awareness would be presented to encourage and inspire the youth to combat cyber security challenges.
- According to a recent Kaspersky survey, Bangladesh is at the top of the list of countries at risk of ransomware Trojan attacks. According to the survey, 3.69% of Kaspersky users in Bangladesh are victims of Trojan attacks, the highest rate in the world. Bangladesh ranked 83rd in the National Cyber Security Index (NCSI) published by Estonia in 2019, but advanced to 33rd in 2022. Following Bangladesh, the highest percentages of Trojan-affected users were reported in Haiti (1.79%), Sudan (1.69%), Turkmenistan (1.41%), Palestine (1.33%), Yemen (1.10%), Tajikistan (1.03%), China (1.01%), Ethiopia (1%), and Pakistan (0.87%).
- Mysterious Team Bangladesh (MT), a hacktivist group targeting Indian government websites and servers, has been discovered by CloudSEK, an AI-powered cyber intelligence and threat detection company. The attacks resemble those launched by DragonForce in early 2022. The threat actor is primarily motivated by hacktivism and

has ties to the Indonesian hacktivist group "Hacktivist of Garuda." They have also been involved in mass reporting of content across public platforms such as YouTube, Facebook, and LinkedIn. CloudSEK concluded that Mysterious Team used the Raven Storm tool for DDoS attacks. The tool employs multithreading to send multiple packets at the same time in order to bring the server down.

SRI LANKA

- Anonymous employed distributed denial-of-service (DDoS) attacks on the websites of the Ceylon Electricity Board, the Sri Lanka Police, and the Department of Immigration and Emigration on April 20. Anonymous claimed to have established the #OpSriLanka hashtag in favour of the people and was "declaring cyberwar against the government" on Twitter. Many Sri Lankans had been calling for the group to step in, using the hashtag #AnonymousSaveSriLanka on social media. But as part of the attack, Anonymous hackers publicly shared thousands of usernames, passwords, and email addresses from the database of Sri Lanka Scholar, a private portal that connects students to various higher education institutions and uses the official ".lk" domain. This has raised questions amongst both cybersecurity professionals and the broader public, as to whether Anonymous is doing more harm than good while showing its support for the anti-government protests.

Disclaimer: Views expressed in MP-IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the MP-IDSA or the Government of India.

Published by:
MP-IDSA Cybersecurity Centre of Excellence,
Manohar Parrikar Institute for Defence Studies and Analyses,
1, Development Enclave, (near USI), New Delhi, Delhi 110010
Email: iccoe.idsa@gov.in

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