MANOHAR PARRIKAR

idsa

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 2021

AN OVERVIEW OF THE CYBERSECURITY LANDSCAPE IN 2021

The events in the cyber realm in the pandemic ridden 2021 weren't dissimilar to the preceding year. The slight difference was the escalation of new virus variants to wreak havoc in our biological and digital systems. The Covid-19 pandemic altered societies due to rapid digitization and accelerated swing to remote working. This forced organisations to adapt to risky makeshift platforms that required sharing sensitive data with third party and open-source services. These platforms are filled with vulnerabilities and hence, pandemic exacerbated the cybersecurity crisis. With the value of digital commerce bound to grow by $800 billion by 2024, organisations have understood the urgent need for securing their digital transformation from malicious actors. The year also showcased the glaring inequalities in the allocation of digital resources. With 40 per cent of the world population yet to get access to the internet, the rapid digitisation is bound to expose new participants to the dangers of the digital world. Therefore, the governments and other stakeholders have a larger role to play.

According to the World Economic Forum's (WEF) Global Cybersecurity Outlook 2022, ransomware, social engineering, and malicious insider activity were the top three cyberattacks organisations are most concerned about. The pace of securing cyberspace hasn't been able to catch up with the cybersecurity threats with malware and ransomware attacks increasing by 435% in 2021. Undiscovered vulnerabilities due to cloud-based digitisation of systems, deficiencies in cyber governance, and pugnacious incentive-driven tactics (facilitated by cryptocurrencies) by threat actors are some of the reasons for increase in cyberattacks.

SURGE IN ATTACKS ON CRITICAL INFRASTRUCTURE

This year also saw breakdown of critical infrastructure due to persistent ransomware attacks. There were attacks across the world on critical infrastructure like SolarWinds, Colonial Pipeline, Irish Health Service, Indian National Electricity Grid and seaports, Indian Smart City servers, Transnet, and Iranian centralised fuel distribution system. Taking into account the drastic increase in cyber-attacks on Indian critical infrastructure, the Indian government has taken a few steps to address the issue. After setting up six sectorial CERTs for Thermal, Hydro, Transmission, Grid Operations, RE and Distribution, the Central Electrical Authority released guidelines to secure the electrical grid and associated infrastructure against cyber-attacks. Furthermore, the Indian government is in the process of setting up a unified national-level cyber security task force with specialised sub-level task forces within it to focus on priority sectors. The first sub-level taskforce is expected to be set up in the telecom sector which is already in the throes of change with the impending shift to 5G.

SPYWARE THREAT

The year 2021 also witnessed the use of spyware by state and non-state actors on journalists, civil rights activities, and political opponents all around the world. This spurred a debate on the current threat to the privacy of individuals. Governments all across the globe had to take a deep dive into their privacy policies. Last year saw at least 75 cases of cyber espionage attributed to threat actors allegedly supported by countries like China, Russia, Iran, and North Korea. Cyberattacks involving spyware are clearly more rampant than ransomware attacks. The utility of cyber espionage ranges from getting information for political objectives to stealing intellectual property of the private and public sector of a country.

PANDEMIC ESPIONAGE

As the pandemic dawned into its second year, cyber-attacks pertaining to stealing Covid-19 related information were widespread. There were media reports of North Korean hackers trying to break into the systems of Pfizer, a pharmaceutical company that produces Covid-19 vaccines. Meanwhile, some Portuguese-speaking cyber criminals gained access to the computers of Oxford University researchers involved in researching the Covid-19 vaccines. The Russian and Chinese intelligence agencies were accused of targeting the European Medicines Agency in 2020 in an attempt to steal data on Covid-19 medicines and vaccines. Interestingly, the Lithuanian government stated that certain Russian hackers were using the country's IT infrastructure to carry out cyber espionage on organisations dealing with the Covid-19 vaccine. Finally, the Chinese allegedly overwhelmed the Australian government's network following Australia's backing of an 'independent international probe' on the 'origins of the coronavirus'.

DISINFORMATION CAMPAIGNS

Apart from a spike in ransomware attacks and cyber espionage, the use of cyberspace to spread disinformation was on a rise. Threat actors use disinformation to spread panic to achieve political objectives during critical and sensitive times. Most of the media reports were on Russian and Iranian hackers using system vulnerabilities to spread disinformation. The Russian hackers supposedly hacked Poland's National Atomic Energy Agency and Health ministry website to spread false alerts of a non-existent radioactive threat according to the Polish security services. Ukraine's Ministry of Defence also claimed that their navy's website was attacked by Russian hackers to publish fake reports on the International Sea Breeze 2021 military drills. Then there were investigations on an expansive disinformation campaign by the Iranian government targeting Israeli activists using WhatsApp and Telegram to 'instigate political unrest' in Israel. With regards to India, Indian Prime Minister, Narendra Modi's Twitter account was hacked to spread fake news regarding Bitcoins. The tweet stated that the Indian government had accepted Bitcoins as a legal tender which included a scam link that promised Bitcoin giveaways. With the advancement in deepfake technology, the significant issue of combating disinformation is a challenge to the policy community.

CYBERCRIME ON RISE

The inescapable demand of digitisation has propelled the 'traditional organised criminal gangs' to use cyberspace to commit crimes. These gangs hire hackers to commit crimes on their behalf. The Darkweb is a fertile ground for such activities and agreements to take root. From extortion to drug trafficking, these gangs run their criminal businesses like an e-market platform on the Darkweb. However, this year also saw many successful busts by several law enforcement agencies against cybercrime syndicates. The Southeast Asian law enforcement agencies in Operation Haechi-I intercepted $83 million over the course of six months from September 2020 to March 2021. Then the Tor-based market on the Dark Web called ‘Slilpp’ was shut down due the international cooperation between the FBI and European law enforcement agencies. Slilpp was responsible for dealing in stolen credentials on the dark web. In 2021, around 281.5 million people were affected by data breaches and such cybercrimes cost companies $4.24 million per incident. Therefore, the shutdown of Slilpp was a great achievement as it had offered its users access to as many as 1,400 websites and 80 million account credentials. Additionally, in a joint operation by Australia and the FBI, more than 800 suspected cyber criminals were arrested worldwide after being tricked into using an FBI-run encryption messaging app called ANOM. The INTERPOL along with law enforcement agencies from over 20 countries carried out an operation arresting over 1000 individuals and seized more than $27 million worth of illicit funds. Although these are positive interventions, the detection and prosecution of organised cybercrime is estimated to be as low as 0.05 per cent in the US. According to India’s National Crime Records Bureau’s 2019 cybercrime data on metropolitan cities- 1342 people were arrested, 1387 were charge sheeted, 163 were convicted, 2 discharged, and 170 were acquitted.

RANSOMWARE EVERYWHERE

In terms of evolving trends, ransomware stirred up a storm everywhere with around 270 attacks per organisation on an average and 100 different strains of ransomware circulating around. This led to the price of cyber insurance soaring to an all-time high. In 2021, the price of cyber insurance cover grew by 130 per cent and 92 per cent in the US and UK respectively. Last year especially saw grave disruptions in the digital supply chains due to ransomware attacks. This greatly affected businesses and critical infrastructure. For example, REvil, a ransomware threat actor, hampered the supply chain affecting 1,500 companies. Furthermore, along with ransomware attacks, the log4j vulnerability discovered in December of last year showcased the challenges of using third-party platforms, open-source software, and task monitoring services. There were over 600,000 attempts to exploit the log4j vulnerability, mostly from hackers from China, Iran, and North Korea. The breaches witnessed from third party services have increased from 44% to 61% in 2021. These complex integrated platforms pose concealed challenges and zero-day vulnerabilities waiting to be exploited.

TAMING CRYPTOCURRENCIES

Many would say that the exponential spike in the ransomware attacks were facilitated by the use of cryptocurrencies. Governments all around the world are struggling to regulate cryptocurrency. The Government of India is planning to introduce a bill to regulate cryptocurrencies under the ‘Cryptocurrency and Regulation of Official Digital Currency Bill’ aiming to create a framework for the creation of an official digital currency in the country and imposing a ban on private cryptocurrencies. In the US, the Biden administration took steps to expand sanctions to digital payment systems involving cryptocurrencies due to the ransomware menace. The first of these measures were to impose a ban on virtual currency exchange called

Suex that had facilitated transactions linked to ransomware. The control of the cryptocurrencies is a tough conundrum due to its evolving nature.

Emerging Technologies and Cyberspace

With the evolution of a more decentralised yet hyper-interconnected Internet 3.0 in cyberspace, emerging technologies, while generating many opportunities, will also pose a grave threat to the security of our digital systems. Technologies like Artificial intelligence (AI), Internet of Things (IoT), Blockchain, cloud computing and 5G are already creating an impact on several operations in cyberspace. It is the Metaverse, Non Fungible Tokens (NFTs), Quantum, and Deepfake emerging technologies that will disrupt the way cyberspace operates. It might become more difficult to identify and rectify newer cyber risks since we will have to use these emerging technologies to counter already existing technologies, further complicating trust in digital and patchwork governance. For example, a study by Capgemini found that two third businesses believe that AI is essential to 'identify and counter' critical cybersecurity threats. The report also stated that three fourths of the businesses were using and testing AI for this reason. The proliferation of IoT and Digital Twining is inevitable with the number of connected devices likely to reach 18 billion by 2022. Hackers now have countless nodes to gain access to any network. According to a report, 48 per cent participants said that automation and machine learning are the biggest transformation forces for cybersecurity. There are also concerns of use of quantum computing to break encryption keys used by critical infrastructures to protect data and conduct communication. Finally, with the inception of metaverse, and accrual of digital assets like cryptocurrencies and NFTs, the cybersecurity policymakers will have to explore uncharted territory.

India's Cyber Governance

The most conventional response to solving all that is not right with cybersecurity is- Cyber Governance. The governments and international organisations dealing with cybersecurity face many challenges that have varying ramifications. India undertook several measures to address these issues. Keeping digital inequality in mind, the Union Cabinet gave approval for setting up the Public Wi-Fi Networks through the Prime Minister Public Wi-Fi Access Network Interface (PM-WANI) scheme. This will help proliferation of public Wi-Fi in efforts to create a vibrant and digital India. In terms of cyber capabilities, it is estimated there is a deficit of 3 million cybersecurity professionals worldwide. India faces a similar issue. Therefore, the All India Council for Technical Education (AICTE) along with the Ministry of Education, and other partners embarked on a mission to skill 5 lakh students in the country in cybersecurity. In the matter of disinformation, the Ministry of Electronics and Information Technology (MeitY) notified the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 (Rules). These rules cover social media platforms, messaging services, OTT platforms and news portals. The rules aim to maintain a 'delicate balance between freedom of speech and expression and reasonable restrictions that uphold national sovereignty and security considerations.' Meanwhile, in a much needed measure, the Ministry of Home Affairs (MHA) operationalised the helpline number 155260 as a reporting platform for financial losses due to cyber fraud. The helpline has been made operational by the Indian Cyber Crime Coordination Centre (I4C) in cooperation with the Reserve Bank of India (RBI).

The National Cyber Security Co-ordinators office also initiated a number of programs including the *Indian Citizen Assistance for Mobile Privacy and Security* (ICAPS) program where the objective was "to build an integrated server system, which can collate all the mobile security-related information and provide customized and actionable knowledge to individual Indian citizens to secure their mobile devices and data on those devices."

INDIA'S INTERNATIONAL CYBER ENGAGEMENT

India also took huge strides in terms of her international engagement on cyber related discussion and partnerships. The Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India signed a memorandum of understanding with Kaspersky to collaborate on cybersecurity. The primary role of CERT-in has been to raise security awareness among the Indian cyber community and provide technical assistance to them. The partnership will also see the execution of joint projects aimed at supporting and accelerating the development of Indian start-ups in the cyber domain, through Kaspersky Innovative Arm- Kaspersky iHub. In the month of June, during the G7 summit, Indian Prime Minister, Shri Narendra Modi referred to India's civilizational commitment to democracy, freedom of thought and liberty. He highlighted the "revolutionary impact" of digital technologies on social inclusion and empowerment in India. He warned about the "inherent vulnerabilities" in open societies and stressed on "ensuring a safe cyber environment" on social media platforms. Keeping in spirit the importance of cyber diplomacy, the Ministry of External Affairs had the following engagements: 1) India-Australia Joint Working Group on Cyber Security Cooperation 2) India-UK Joint Working Group on Cyber Capacity Building 3) India-France Cyber Dialogue 4) India-New Zealand Bilateral Cyber Dialogue 5)India-UK Working Group on Cyber Deterrence 6) RATS SCO Practical Seminar on Securing Cyberspace in the Contemporary Threat Environment.

CYBER WARFARE AND NORM-BUILDING

In the midst of superpower tussle, cyberspace is yet another battlefield to assert dominance. In terms of international organisations and dialogues, there is a clear shift in groupings-based cooperation and discourse setting rather than IOs like the United Nations influencing the norms around cyber governance. This clearly indicates a divide and difficulty in agreeing to universal norms for cyber governance. Nonetheless, the UN Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), submitted its report in March 2021 while the parallel running UN Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in context of international security's report was adopted by consensus in June 2021. This was an encouraging step in norm and consensus building but there is much left to achieve. In terms of dialogues between various groupings, the Australian Department of Foreign Affairs and Trade (DFAT) has allocated AUD 497,000 for a QUAD Tech Network project under QUAD. The move aims at strengthening the cooperation between the QUAD countries namely- Australia, US, Japan, and India, on cyber and critical technology issues. The QUAD also issued a joint statement on critical and emerging technologies in September for 'promoting the free, open, rules-based order, prosperity in the Indo-Pacific and beyond'. Interestingly, in addition to the acquisition by Australia of nuclear-powered submarines, the new AUKUS trilateral security pact between Australia, the UK, and the US, announced that they will also focus on cyber capabilities, AI, and quantum technologies as a means to enhancing undersea and military capabilities. Lastly, the US-EU Trade and Technology Council (TTC) meet took place in September. The TTC is a new forum with ten working groups to discuss various issues, including sensitive technologies, boosting semiconductor production, addressing chip shortages and also the regulation of large technology firms. The Information and Communications Technology and Services working group was tasked to continue to work towards ensuring security, diversity, interoperability, and resilience across the ICT supply chain, 5G and beyond, undersea cables, data security and cloud infrastructure.

SECTORAL ANALYSIS OF KEY CYBERSECURITY INCIDENTS IN 2021

CRITICAL INFRASTRUCTURE

In the month of March, there were reports of Chinese hackers targeting Indian electricity grids in an attempt to gather information and find vulnerabilities for possible future attacks. Interestingly, the Indian Computer Emergency Response Team found evidence of Chinese hackers conducting a cyber-espionage campaign against the Indian transportation sector. The US witnessed many attacks on its critical infrastructure. There was an attempt by hackers to raise levels of sodium hydroxide in the water supply of Oldsmar, Florida. The Chinese hackers allegedly targeted New York City's Metropolitan Transportation Authority, Metropolitan Water District of Southern California, and various other government agencies and oil/natural gas pipeline companies according to media reports the entire year. Additionally, Russian hacking gangs like DarkSide and REvil, targeted Colonial Pipeline (largest fuel pipeline in the United States), Sol Oriens (government contractor that works for the Department of Energy on nuclear weapons), and several other facilities.

In Europe, Ireland's national health service, the Health Service Executive (HSE), was the victim of a ransomware attack in May apparently attacked by a Russian-based cybercrime group. Then the Norwegian energy technology company, Volue was the victim of a ransomware attack in May which resulted in the shutdown of water and water treatment facilities in 200 municipalities, affecting approximately 85% of the Norwegian population. Belgium witnessed two cyberattacks on its critical infrastructure throughout the year- a DDoS attack that disabled the ISP used by the Belgian government affecting cancellation of multiple Parliamentary meetings and a cyberattack on the Belgium Ministry of Defence computer networks due to log4j vulnerability.

In the Indo-Pacific region, South Korea's state-run Korea Atomic Energy Research Institute (KAERI) witnessed a cyberattack allegedly by North Korean hackers using a vulnerability in a vendor's VPN. According to a Bloomberg investigation, there was an intrusion in Australia's telecommunications systems in 2012 due to a malicious code embedded in a software update from Huawei. In West Asia, Iran's transport and urbanisation ministry was the victim of a cyberattack that caused delays and cancellations of hundreds of trains around the country. In Saudi Arabia, hackers gained access and demanded a $50 million ransom to be paid failing which they would release over 1 terabyte data of an oil company extracted using a zero-day exploit. In the African region, South Africa's Transnet Port Terminals (TPT), a state-run ports operator, was hacked disrupting the many associated services..

POLITICAL ESPIONAGE

Cyberattacks pertaining to political espionage continue to be the most common form of espionage with the hotspots replicating what was happening in inter-state relations offline. 2021 witnessed most of the political espionage reported from threat actors from China, Russia, Iran, and North Korea. In July, there was reporting of many countries using Pegasus, a spyware created by Israeli NSO Group, used to target operating systems of activists, politicians, and journalists. There were also reports of the Chinese military conducting a surveillance campaign against Tibetans and Chinese hackers apparently used Facebook (now Meta) to send malicious links to Uyghur activists and journalists abroad in an attempt to hack them. The Chinese threat actors launched a dedicated espionage campaign to target and gain critical information from several Southeast Asian countries, especially nations engaged in disputes on territorial claims in the South China Sea. In a widespread Advanced Persistent Threat (APT) operation by the Chinese entities, researchers found around 100 victims from Myanmar and 1,400 from the Philippines. Additionally, multiple Chinese hacking groups were responsible for the intrusion of at least five major Southeast Asian telecom providers linked to espionage attempts from China. China linked cyber espionage groups reportedly penetrated the network supporting the Afghan National Security Council using phishing emails. It was also found out that Norway attributed the cyberattack on their parliament's email system to China. The Norwegian Government stated that 'bad actors sponsored by and operating from China' had attempted to capture classified information related to Norway's national defence and security intelligence. And in the twist and turns common to cyber attack reporting, cyberattacks on Israeli government and tech companies which were first attributed to Iran were actually found to have been conducted by Chinese threat actors. Finally, the US, European Union, NATO, and several other world powers released a joint statement blaming the Chinese government of the Microsoft Exchange hack that compromised more than 100,000 servers worldwide.

There were several media reports on the Ukraine-Russia cyber conflict. In February, Ukrainian officials reported that a DDoS attack against the Ukrainian Security Service was part of Russia's hybrid warfare operations in the country. Then in the month of March, Ukraine's State Security Service announced it had prevented a large-scale attack by Russian FSB hackers attempting to gain access to classified government data. Various European countries accused Russian hacking groups of cyber espionage. In April, the Swedish officials stated that the Swedish Sports Confederation was hacked by Russian military intelligence due the Russian government-sponsored doping of Russian athletes controversy. There were also news reports in June that Russian intelligence services hacked Netherlands police internal network during the country's investigation of the Malaysia Airlines Flight 17 (MH17) that was shot down in 2014. Cyberattacks on the Polish and Slovak government were attributed to Russia. Russian hackers allegedly stole thousands of emails after breaching the email server of the U.S. State Department. Finally, Russian-speaking groups targeted the personal information of around 3,500 individuals that included government officials, journalists, and human rights activists using malware on Android and Windows devices.

In West Asia, Iranian threat actors appeared to be more persistent according to media reports. In February, there were three different reports on Iranian hacking groups conducting espionage campaigns against Iranian dissidents in sixteen countries, and government agencies in the UAE due to its normalizations of relations with Israel, with hackers also taking control of a server in Amsterdam and used it as a command and control centre for attacks against political opponents in the Netherlands, Germany, Sweden, and India. In March, suspected Iranian hackers carried out a cyber-espionage campaign targeting government agencies, academia, tourism industry, medical researchers from Azerbaijan, Bahrain, Israel, Saudi Arabia, UAE, and the US. Similar to Chinese tactics, Iranian hackers also allegedly used Facebook to pose as recruiters, journalists, and NGO affiliates, targeting U.S. military personnel. Interestingly, in August, a hacking group targeted an important Iranian prison, uncovering data that displayed the violent treatment of its prisoners. Anonymous hackers leaked 11 terabytes of data from the Israeli Defense Ministry after gaining access to 165 servers and 254 websites in October. With regards to conflicts, hackers from Palestinian intelligence conducted a cyber-espionage campaign on 800 Palestinians in April and cybersecurity researchers found a mobile espionage campaign against the Kurdish ethnic group in September.

In May, according to a few news reports, a North Korean hacking group was responsible for a cyber-espionage campaign, targeting high profile South Korean government officials through phishing techniques. Threat actors linked to the Vietnamese government conducted a nearly three-year cyber espionage campaign against several human rights advocates. Additionally, Fujitsu's network was intruded by hackers to steal data belonging to multiple Japanese government entities. In cyber espionage attacks that are yet to be attributed, a spreadsheet was leaked containing classified personal details of the 1,182 United Kingdom's Special Forces soldiers on WhatsApp in July. Further, there was an attempt to hack the UK Labour Party data affecting personal data of its members. Finally, a cyberattack against the United Nations occurred in April 2021 with the objective of long-term intelligence gathering. Shockingly, hackers were able to access their network through credentials obtained through the dark web.

INDUSTRIAL ESPIONAGE

With growing complexity and blurred lines on cyberattack objective and intent, the gap between Political and Industrial Espionage has reduced. Protection of business is part of a country's national security wellbeing. The year 2021 witnessed a huge jump in the Industrial Espionage cases. With reference to various accusations pointing to Russian threat actors, in February, the French National Cybersecurity Agency stated that Russian hackers had run a four-year campaign targeting French IT companies. Then the Russian Foreign Intelligence Services were accused of installing malicious software on the Microsoft Office 365® system to access millions of account information in June. The Chinese hackers too were accused of hacking targeted Microsoft's enterprise email software to steal data from over 30,000 organisations. The Chinese hacking groups apparently took great interest in US defence contractors with multiple reports of penetration attempts in April, November, and December. China-based threat actors also compromised a Russian defence contractor involved in designing nuclear submarines for the Russian navy and Afghan telecom provider Roshan according to multiple sources. Interestingly, the Chinese government claimed that foreign intelligence agency hacked into several airlines in China and stole passenger information.

In February it was revealed that since 2020, North Korean hackers have targeted defence firms in more than a dozen countries and they were also responsible for hacking several cybersecurity researchers in January. Finally, in attacks that are yet to be attributed, several members of a cyber-criminal gang were arrested after they duped telecom companies into assigning celebrities' phone numbers to new devices, stealing more than $100 million worth of cryptocurrencies. In March, the Australian media company Nine Entertainment was targeted through a ransomware attack, disrupting broadcasting.

ELECTORAL PROCESSES

The year started with the head of US Cyber Command testifying that the organisation had conducted several operations to address foreign threats for the US elections in November 2020. The US Cyber Command also stated that they were helping Columbia to address the issues of 'election interference and influence operations.' In March, Russian hackers allegedly attempted to enter personal email accounts of several German parliamentarians just before Germany's national elections. Additionally, Russia blocked the "smart voting" app created by Alexei Navalny, a critic of the Russian government. The app aimed to organise voting for Russia's parliamentary elections. Hungary witnessed a cyberattack on its polling systems in electoral districts nationwide two hours after the voting opened for Hungary's opposition primary elections in September. Finally, in the same month, the EU accused Russia of its involvement in targeting the elections and political systems of several member states. This campaign was named as the 'Ghostwriter' cyber campaign where Russian operators hacked the social media accounts of government officials and news websites, with the goal of creating distrust in US and NATO forces.

MAJOR CYBER INCIDENTS IN THE SOUTH ASIAN REGION

INDIA

The Indian Government imposed fresh notices for the permanent ban of TikTok and 58 other apps from Chinese companies after they failed to provide satisfactory explanation to the government with regards to the privacy and security of data collection by them. The apps were earlier banned by the government in June 2020.

The Reserve Bank of India (RBI) has taken steps to look into matters related to enforcement of new payment aggregator licensing norms, following cyberattacks on Indian payments companies like Juspay. Juspay had confirmed the August 2020 data breach after an investigation revealed unauthorised access by hackers on a server that formed part of its payment system. The data breach affected 35 million customer accounts with masked card data and card fingerprints.

In yet another incident of data breach just two months after the Juspay breach, a cyber-security researcher claimed in March that user data that included sensitive information of 3.5 million users of Mobikwik, a payment company, were put up for sale on the dark web. The details included KYC information, addresses, phone number, Aadhar card numbers, etc.

The servers of a smart city, the Pimpri Chinchwad Municipal Corporation in Pune were hit by a ransomware attack in February. The smart city project is managed by the multinational technology company, Tech Mahindra. Although there was no data loss in the attack, the hackers have reportedly demanded the ransom to be paid in bitcoins.

Data from the 2020 breach of online grocery delivery platform BigBasket, was allegedly leaked on the Dark Web in April 2021. The data contained details of over 20 million customers which included email addresses, names, date of birth, hashed passwords and phone numbers. A hacker group known as ShinyHunters was behind this attack.

In May, two high profile hacks of Air India and Dominos were reported. The attack on Air India exposed personal data of around 4.5 million passengers. In the Dominos India hack, sensitive information like phone numbers, names, and payment information of around 18 million orders was put on sale on the dark web.

PAKISTAN

The federal cabinet of Pakistan approved the National Cyber Security Policy 2021 that would allow establishment of a national cyber security response framework for implementation of cybersecurity policies in the country. The Cyber Governance Policy committee constituted under the framework will be responsible for implementing the policy at the national level.

In October, the National Bank of Pakistan (NBP) was the target of a cyberattack. The bank, on the other hand, informed its customers that no financial information had been exposed and that no data breach had occurred. Cyberattacks had previously targeted Pakistan's Federal Board of Revenue (FBR) database. Every month, on average, 71,000 cyberattacks were launched against the FBR portals.

The national security advisers of Pakistan and Russia met in Moscow in December to discuss bilateral cooperation in the domains of economy, energy, defence, counter-terrorism, counter-narcotics, information, and cybersecurity. Collaboration between law enforcement agencies, special services, and defence ministries was also discussed between the two parties.

BANGLADESH

In November, the Bangladesh Bank stated that they were going to launch a computer emergency response team for the financial sector (Fin-CERT) to avert cyber-attacks. This step is taking into consideration the biggest digital heist in the country’s banking history, when hackers were able to syphon off $81 million from its accounts with the Federal Reserve Bank of New York in 2016.

That apart, Bangladesh ranked 38 among 160 countries in the latest iteration of the National Cyber Security Index (NCSI) brought out by the eGovernance Academy Foundation, Estonia. The index is prepared on the basis of an analysis of the cyber security and digital development in the participating countries. It is a dynamic index with rankings revised several times a year based on developments in the respective countries. The Index acts as a benchmark for countries to make an assessment of their cybersecurity preparedness.

SRI LANKA

For the Colombo Conclave, at the Deputy National Security Adviser level meeting hosted by Sri Lanka on August 4, marine safety and security, terrorism and radicalisation, trafficking and organised crime, and cybersecurity were identified as the "four pillars" of cooperation. The trilateral security meeting between Sri Lanka, India and Maldives was held virtually. Bangladesh, Mauritius, and Seychelles participated as Observers.

In October, the Sri Lankan Cabinet approved recommendations to write two cyber security bills targeted at combating terrorist groups and criminals who use cyberspace and electronic communication for anti-social purposes. In his dual role as Minister of Defence and Ministry of Technology, President Gotabaya Rajapaksa proposed drafting a bill titled "Defense Cyber Commands Act " and a bill establishing cyber protection regulations.

NEPAL

According to the International Telecommunication Union, Nepal has moved up to 94th place in the Global Cybersecurity Index 2020 from 106th place in the 2018 edition, indicating that its commitment to cybersecurity has risen (ITU).

The Ministry of Communication, Information and Technology has drafted National Cyber Security Policy 2021 to regulate and mitigate cyber-attacks in the information and technology sector, as well as offer security against future attacks.

BHUTAN

Bhutan became the first country to use India's Unified Payment Interface (UPI) standards for its QR code in July. Union Finance Minister Nirmala Sitharaman and her Bhutanese counterpart Lyonpo Namgay Tshering introduced BHIM-UPI in Bhutan in a virtual event. Bharat Interface for Money (BHIM) is an India-based digital payment system that uses UPI, an immediate real-time payment mechanism. Multiple bank accounts can be accessed using a single mobile application using the UPI.

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