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 2023

AN OVERVIEW OF THE CYBERSECURITY LANDSCAPE IN 2023

The year 2023 witnessed a consistent increase in cyber incidents, following similar trends to the previous year. As technology advances rapidly, these cyber incidents become more sophisticated, thereby heightening vulnerabilities in the cyber domain. A study found that as automation increases, enemies and defenders are progressing at different speeds; while attackers are quickly adapting to the advancements in technologies, defenders are unable to keep up. Similar advancements have also led to the widening of attack surface, leading to cyber attacks of varying scales.

In 2023, geopolitics had a greater impact on the cyber domain, as seen by the rise in cyber incidents linked to political events of the time. The ongoing Ukraine-Russia conflict continues to affect cyberspace, which is evident as both sides intensify their attacks on one another. Similar trends could be observed in the current conflict between Israel and Hamas, demonstrating the conflict's modern hybrid nature.

There was a global fervour surrounding Artificial Intelligence (AI), with enthusiasts and sceptics discussing the technology's future with equal enthusiasm. The conversation about rapidly evolving technologies such as AI encompassed a wide range of participants who readily exchanged thoughts, worries, and mutual interests regarding intelligent systems and their future. Despite the debate on regulation, which usually falls under the remit of governments, multi-stakeholder platforms were convened to discuss the future of technology and explore ways to utilize it more effectively and with lesser risks. Some of these initiatives included the REAIM summit, the first global summit on Responsible Artificial Intelligence in the Military Domain; the Bletchley Declaration on AI safety; and the Global Partnership on Artificial Intelligence (GPAI), to name a few.

The cybercrime ecosystem is on a steady rise, as cybercriminals are leveraging the cybercrime-as-a-service ecosystem to launch phishing and distributed denial of service (DDoS) attacks at scale. Threat actors are reportedly exploiting cloud computing resources like virtual machines to launch DDoS attacks. Other tools and techniques employed include business email compromise (BEC) attacks. Furthermore, cybercriminals continue to exploit legitimate remote monitoring and management (RMM) software for malicious activities. Regarding ransomware, the situation seems increasingly dire despite efforts by nations to rally support against such attacks. An alarming statistic reveals that in 2023, 1 in every ten organizations globally experienced attempted ransomware attacks, marking a 33 percent increase from the previous year.

The cyber insurance industry continues to grow in response to the escalating risks and liabilities associated with cyber incidents, as an increasing number of governments consider imposing substantial penalties following data breaches. In 2022, the global cyber insurance market's annual premiums reached about $12 billion, and this figure is expected to rise to about $23 billion by 2025. This steady increase in cyber insurance adoption is primarily due to the rise in the cost of data breaches. In 2023, the average cost of a data breach soared to a record $4.45 million, marking a 2.3% rise from the 2022 figure of $4.35 million.

There were mixed signs concerning blockchain technology and its prominent application in cryptocurrencies. The collapse of the FTX exchange dominated the news cycle, overshadowing other developments. Meanwhile, Sam Altman, the CEO of OpenAI, launched a novel blockchain initiative called Worldcoin, aiming to build a biometric database of the human population in exchange for giving them access to crypto and a digital ID.

According to forecasts, policymakers have to brace for a challenging period in 2024. Geopolitical realities will play a crucial role in shaping the cyber domain and will continue to significantly influence decision-makers. Concerns regarding the weaponization of Generative AI and Large Language Models (LLMs) will dominate the decision-makers, encouraging more discussions around regulation.

ARMED CONFLICTS AND CYBER REALM

The conflict in Ukraine continues to influence the cyber domain, as both sides actively engage in efforts to undermine each other in cyberspace. This trend highlights the hybrid nature of modern conflicts, which increasingly extend into the cyber realm. The challenge of attributing cyber attacks, often compounded by the use of proxy actors in cyberspace, has made it advantageous for state actors to involve non-state entities. This was particularly evident in 2023 with the emergence of 'hacktivist' groups like Anonymous Sudan and others.

Russia-linked threat actors have been pivotal in conducting influence operations and various other cyber activities. Even after the death of Prigozhin, the Internet Research Agency, which is linked to him, had continued its relentless operations. Reports indicate that these Russian-affiliated actors have focused their efforts on intelligence collection from Ukrainian communications and military infrastructure. They have also employed various Tactics, Techniques, and Procedures (TTPs) to boost influence operations. Furthermore, the groups have also been targeting the diaspora along with launching attacks to target the Ukrainian energy and agricultural sector.

Russia had also been at the receiving end of cyber attacks, some orchestrated by hacktivist collectives in support of Ukraine and others by Ukrainian government agencies. These attacks have revealed that the Russian cybersecurity defences are considerably weaker than previously assumed. Hacktivist groups like Anonymous have targeted Russian databases and companies that continue to engage in business with Russia. They have also disrupted websites through DDoS attacks. According to reports, Ukrainian cyber-operators have been actively deployed on the front lines to intercept communications of the Russian military. Furthermore, Ukrainian security services have also employed AI-powered visual recognition systems to analyse data from aerial drones to locate military targets. Lately, Blackjack, a Ukrainian group of hackers, have breached 500 Russian military sites, exacerbating the existing tensions in the cyber domain.

In another part of the globe, Israel and Hamas have been engaged in similar tussles in cyberspace. Following the unprecedented attack by Hamas on Israel and the declaration of war

by the latter, both the sides and their supporters and affiliates have been incessantly attempting to undermine each other in cyberspace. Within a week of the attack, pro-Palestinian cyber activities began targeting Israeli entities through DDoS campaigns and website defacements. These attacks covered a wide array of targets, from national infrastructure to political figures. With conflict getting more intense with each passing day, the scope of pro-Palestinian activities expanded beyond Israel, targeting countries perceived as Israeli allies in the conflict with Hamas.

Moreover, due to the nature of the conflict, the cyber frontline widened to involve Iranian-affiliated groups, broadening the impact of the ongoing conflict. Cyber activities linked to Israel are also on the rise, with the latest significant incident being a cyber attack on Iranian gas pumps. This attack disrupted a significant portion of Iran's gas stations, highlighting the escalating nature of the cyber warfare in the region. Across social media platforms, there was a noticeable increase in disinformation or influence operations. These efforts, powered by AI tools, were used to generate fake images and videos, commonly known as 'deepfakes', to sway global opinion.

Similar trends were visible in the Armenia-Azerbaijan conflict, with warring parties employing digital tools to their advantage. As recently reported, Apple warned Armenia of state-sponsored hacking attempts. Some suggested these intrusions were linked to the Azerbaijani government, which had a history of conflict with Armenia over the Nagorno-Karabakh region. The use of spyware, in particular, is making headlines when it comes to the Armenia-Azerbaijan tussle in cyberspace.

MAJOR CYBER BREACHES

In 2023, data security suffered significant setbacks due to numerous major data breaches occurring across continents. One notable breach occurred in India, as reported in the media. According to reports, the Indian Council of Medical Research (ICMR) fell victim to a significant data breach, resulting in the exposure of personal information belonging to over 815 million registered individuals. This compromised data, available for purchase on the dark web, includes crucial details such as Aadhaar and passport information, alongside names, phone numbers, and addresses.

In another significant cyber breach incident, about 2,620 organizations and 77.2 million individuals have been affected by the hacking of the file transfer service MOVEit since May 2023. US-based organizations have experienced the most severe impact, with 78.1 percent of the affected organizations originating from the United States. Following closely behind was Canada with 14 percent, Germany with 1.4 percent, and the UK with 0.8 percent of the affected organizations, according to reports. The majority of impacted organizations hailed from the education sector, accounting for 40.6 percent of the total, followed by the health sector at 19.2 percent and finance and professional services at 12.1 percent.

In November 2023, internal data from Boeing, one of the world's largest defence and space contractors, was published online by Lockbit, a cybercrime gang known for extorting its victims by stealing and releasing data unless a ransom is paid. The company later confirmed the breach in a statement.

As a consequence of these cyber breach incidents, the cost of data breaches had also escalated. According to IBM's Cost of a Data Breach Report 2023, the global average cost of a data breach in 2023 amounted to USD 4.45 million, reflecting a 15 percent increase over the span of three years.

RELENTLESS RANSOMWARE

Ransomware attacks have shown no signs of abating and have grown manifold in the last few years. Checkpoint research declared 2023 as the year of "mega ransomware attacks", providing a detailed analysis of the threat landscape for the entire year. The report noted that unlike traditional ransomware attacks that focus on encrypting victim's data and demanding ransom for its release, there was a shift in tactics by cybercriminals in 2023. These criminals concentrated more on stealing data, followed by extortion campaigns that did not necessarily involve data encryption but rather threats of public disclosure of the stolen data. According to the same assessment, in 2023, 10 percent of organizations globally were targeted by attempted ransomware attacks, marking a significant increase from the previous year, when 7 percent of organizations faced similar threats.

Looking at the industry-specific ransomware trends, education and research-related organizations were the most targeted sectors. Notwithstanding steady rise in ransomware activities, attacks across several sectors dipped slightly in December. Threat actors also faced setbacks on several occasions due to proactive measures taken by various governments and law enforcement agencies worldwide. A collaborative effort by multiple law enforcement agencies across the globe led to the dismantling of the Qakbot network, which was used for ransomware attacks and scams. In a separate operation, the FBI and Europol successfully took down the Ragnar Locker ransomware site. In another incident, the pro-Ukrainian hackers claimed responsibility for wiping the servers of the Trigona ransomware gang, a group suspected of having ties with Russian cybercriminal underground.

India emerged as a major target for ransomware attacks by threat actors. A survey revealed that nearly 73 percent of mid to large-sized organizations in India experienced a ransomware attack in 2023.

AI AND DEEPFAKES

The latter part of 2022 saw the rise of OpenAIs ChatGPT platform, sparking much discussion, curiosity and apprehension around the technology. However, the observers did not fully anticipate the extent of the impact that such AI-generated tools would have throughout 2023.

This impact was particularly evident in the proliferation of deepfakes. The gravity of the threat posed by deepfakes can be measured by its classification as a top security concern ahead of the 2024 elections. The phenomenon is not limited to the US, spanning across continents. Deepfakes have been used prominently in conflict zones as part of larger disinformation campaigns, notably during the ongoing Israel-Hamas conflict, where AI-enabled disinformation proliferated. In fact, there were instances where Indian celebrities and political leaders had their deepfakes circulating in social media platforms raising concerns about privacy and sanctity of the electoral system respectively. To address this growing concern, Google decided to partner with Shakti, an Indian fact checking collective to help news publishers to detect deepfakes and misinformation.

The increase in AI adoption can also be seen in the cloud environments, with more than 70% of organisations surveyed currently employing managed AI services. However, a significant portion of organizations (32%) seem to be in the experimental stage with these tools, as they deploy fewer than 10 instances of AI services in their cloud environments. According to another assessment, generative AI, despite its nascent phase, is widespread in its usage. This resulted in changes in the types of recruitment in organization with employers hiring data engineers, AI data scientist and prompt engineers, as they aim for integrating AI. Recently, roles in prompt engineering have emerged, as the demand for that skill set increases alongside the adoption of generative AI. According to a forecast for AI related advancements, the year 2024 is going to see some profound changes. In 2024, open-source pretrained AI models gain significant traction, enabling businesses to accelerate growth by integrating these models. The widespread availability of application programming interfaces (APIs) will also streamline the development of AI-driven applications, enhancing productivity across multiple sectors. Given the immense potential of AI, nations worldwide are going to be proactive in development of the intelligent systems. There will also be a heightened focus on AI safety and ethics.

CYBERCRIME ON RISE

The year 2023 saw a significant increase in cybercrime activity. One of the most significant breaches of the year occurred when Chinese hackers infiltrated Microsoft's cloud-based Exchange email platform in May 2023, resulting in the theft of tens of thousands of emails from U.S. State Department accounts. According to reports, the attackers managed to steal at least 60,000 emails from Outlook accounts belonging to State Department officials stationed in East Asia, the Pacific, and Europe.

In another instance, a massive data breach occurred, impacting the country's Immigration Directorate General at the Ministry of Law and Human Rights, resulting in the leak of over 34 million Indonesian passports.

Cybercrime in India saw an increase as well. According to reports, India experienced 129 cybercrimes per lakh population in 2023. Complaints on the National Cybercrime Reporting Portal (NCRP) surged by 61%, reaching 15.6 lakh in 2023 from 9.66 lakh in 2022. However,

this increase was significantly lower than the 113.7% rise observed between 2021 and 2022. In 2023, the cybercrime rate in India, measured by reported cybercrime complaints in the NCRP per lakh population, stood at 129. However, state-wise data indicates that Delhi led with a rate of 755, followed by Haryana at 381 and Telangana at 261. The different categories of cybercrime include customer care scams, refund-based frauds, KYC expiry frauds, sextortion, online booking frauds, AePS frauds, biometric cloning, and various others.

The Central Bureau of Investigation (CBI) announced that it conducted a series of criminal raids in multiple cities across India. This operation was facilitated by a joint referral made by both Microsoft and Amazon. This collaborative referral allowed for the sharing of actionable intelligence and insights between the CBI and other international law enforcement agencies, enabling them to take comprehensive actions. The illegal call centres raided by CBI were set up to impersonate Microsoft and Amazon customer support.

STATE OF CRYPTOCURRENCY AND REGULATIONS

The regulatory landscape for cryptocurrencies underwent significant changes in 2023, with increased scrutiny and regulation. Lawmakers in the EU passed the world's first comprehensive package of rules aimed at regulating the cryptocurrency industry. The EU Parliament approved the Markets in Crypto Assets Act or MiCA. This legislation, designed to mitigate risks for consumers purchasing crypto assets, establishes liability for providers in the event of loss of investors' crypto assets. Platforms will be mandated to disclose information to consumers regarding the risks associated with their operations, and sales of new tokens will also be subject to regulation.

The UK government confirmed its intentions to regulate the crypto industry through formal legislation by 2024. The government's proposals entail implementing stricter regulations for exchanges, custodians responsible for storing crypto assets on behalf of clients, and companies involved in crypto lending. The UK also aims to establish stricter regimes concerning market abuse and the issuance and disclosure of crypto assets.

In January 2023, El Salvador approved a law regulating the issuance of digital assets by both state and private entities. The law aims to attract both national and foreign investors while also creating new financing opportunities for citizens, companies, and the government. It is pertinent to note that El Salvador is the first country in the world to recognize Bitcoin as a legal tender.

According to a report, developing countries are at the forefront of crypto adoption. The Global Crypto Adoption Index ranks India as the leader in crypto adoption, followed by Nigeria and Vietnam. Interestingly, apart from the US, which ranks fourth, the rest of the top 10 list is comprised of developing countries. However, this doesn't imply that crypto is fully accepted at the governmental level in India. In March 2023, it was reported that the government had implemented money laundering provisions on cryptocurrencies or virtual assets, aiming to strengthen oversight of digital assets. In a gazette notification, the Finance Ministry indicated

that anti-money laundering legislation now applies to crypto trading, safekeeping, and related financial services. Following this directive, Indian crypto exchanges will be required to report suspicious activity to the Financial Intelligence Unit India (FIU-IND). Recently, it was reported that FIU issued notices of show-cause to nine offshore cryptocurrency platforms under the stringent Prevention of Money Laundering Act (PMLA). The notices were issued due to non-compliance with anti-money laundering legislation.

A cryptocurrency scam in Himachal Pradesh, India, amounting to Rs 2500 crore, had impacted approximately 5,000 government employees and individuals who had received compensation for their land. Continuing its crackdown against the scam, the special police team (SIT) nabbed eight more persons, taking the arrests to 18. The SIT reconstructed the website involved in the crypto scam having almost 2.5 lakh different IDs.

In the ongoing Israel-Hamas conflict, the Israeli police have taken action to freeze cryptocurrency accounts associated with the Palestinian militant group Hamas. According to reports, the cyber arm of Israel Police's Lahav 433 unit collaborated with the country's defence ministry, intelligence agencies, and the cryptocurrency exchange Binance to target the identified accounts.

CYBERATTACKS ON HEALTH SECTOR

The healthcare sector emerged as a primary target for cybercriminals, with over half of healthcare organizations worldwide experiencing cyberattacks. The worst fears came true when a hospital closure in the US was linked to a ransomware attack. According to observers, this incident marks the first time a hospital publicly attributed its closure to criminal hackers. In the US, as reported, the cyber attacks on hospitals each year doubled between 2016 to 2021. According to US Department of Health and Human Services, ransomware attacks targeting healthcare organizations have surged by 278% over the past four years. According to the agency, the notable breaches reported in 2023 impacted over 88 million individuals, marking a 60% increase from the previous year. Another cyber incident led to the closure of emergency rooms in at least three states, compelling the organization to redirect patients to alternative facilities.

The Indian health sector has also encountered disruptions due to cyberattacks. The All India Institute of Medical Science (AIIMS) in New Delhi experienced cyberattacks for the second time within one year. The premier medical institution reported that the attempted malware attack was effectively repelled, and the threat was neutralized promptly.

STATE OF EMERGING TECHNOLOGIES

In 2023, the top ten emerging technologies under discussion included AI-enabled healthcare delivery, flexible batteries powering wearable medical devices, neural-interfacing flexible circuits, and virtual shared spaces for mental health support. There was an exploration into

spatial omics for molecular-level understanding, engineered viruses for health augmentation, and generative AI capable of creating original content.

While major players like Meta and Microsoft made significant investments in augmented reality (AR) and virtual reality (VR), user adoption did not reach the anticipated heights. However, the realms of AR and VR found their footing in more practical applications, especially in education and training. The growth in Web3 and blockchain technology proceeded steadily and was not as exponential as expected.

The convergence of digital twins and 3D printing in 2023 proved to be a successful fusion. Digital twins are virtual replicas of physical objects or processes, enabling monitoring, analysis, and simulation of real-world entities. Industries ranging from aerospace to healthcare leveraged the capabilities of digital twins for simulation and testing purposes, while 3D printing advanced in material complexity and durability, breaking new ground. The global race for quantum supremacy persisted in 2023, marked by heightened investments, but without any significant breakthrough. The advancement of autonomous systems in logistics and delivery was a notable highlight of 2023. This trend illustrated the increased use of self-driving vehicles and drones, coupled with enhanced warehouse automation. Companies such as Amazon spearheaded this initiative, demonstrating the practical and efficient implementation of autonomous technology in real-world scenarios.

CYBER ESPIONAGE

According to Microsoft, cyberattacks have affected 120 countries, driven by government-sponsored espionage, with a concurrent increase in influence operations (IO). Reportedly, almost half of these attacks were directed at NATO member states, while over 40% targeted government or private-sector entities engaged in the construction and maintenance of critical infrastructure. The espionage operations in the cyber domain were primarily attributed to China, Russia, Iran, and North Korea.

According to another report by Microsoft, since February 2023, Microsoft has been monitoring password spray activity targeting thousands of organizations. These attacks have been attributed to an actor tracked by Microsoft as Peach Sandstorm (HOLMIUM). Peach Sandstorm was identified as an Iranian nation-state threat actor that targeted organizations in the satellite, defense, and pharmaceutical sectors worldwide. Microsoft's assessment, based on the profile of victim organizations and intrusion activities, suggests that this initial access campaign was potentially aimed at facilitating intelligence collection to further Iranian state interests.

In another operation linked to Iran, hackers initiated a cyber espionage campaign, deploying the newly discovered Menorah malware to infect their targets. In one of their campaigns, commencing in August 2023, the hackers employed phishing emails sent to victims presumed to be situated in Saudi Arabia, leading to their infection with the Menorah malware, as per researchers' findings.

According to a cyber threat assessment report published in 2023 outlining North Korea's cyber strategy, the regime is primarily focused on aggressive information gathering and financial theft operations to bolster its broader strategic objectives. The regime engages in information collection to glean insights into the perspectives of its adversaries and to acquire technology that could offer an advantage during periods of conflict. Financial theft is utilized to finance the regime's activities, including its nuclear and missile programs. Espionage remains the primary objective of North Korean cyberattacks.

An assessment published in 2023 uncovered a North Korean cyber espionage operation targeting Russia. A select group of North Korean hackers clandestinely infiltrated computer networks at a prominent Russian missile developer for a duration of at least five months in 2022. According to reports, cyber espionage teams associated with the North Korean government, identified as ScarCruft and Lazarus by security researchers, covertly implanted stealthy digital backdoors into systems at NPO Mashinostroyeniya, a rocket design bureau located in Reutov, a small town on the outskirts of Moscow.

Some cyber-espionage activities targeting embassies and international organizations were traced back to Russian state-sponsored hackers, as discovered by cybersecurity researchers from the Ukrainian government. The attacks were attributed to the notorious hacker group identified as APT29, also recognized as Cozy Bear or Blue Bravo. Analysts have previously linked this group to Russia's Foreign Intelligence Service (SVR), which is known for collecting political and economic intelligence from foreign entities.

CHINESE CYBER ESPIONAGE ACTIVITIES

Chinese affiliated groups have persistently engaged in cyber espionage activities with the objective of acquiring sensitive information from various sectors, including the military. The gravity of the situation is evident from a U.S. Department of Defence (DoD) report to Congress reviewing China's military and security activity. In the report, DoD warned about the growing Chinese activities targeting U.S. government systems, stealing sensitive data from critical defense infrastructure and research institutes. A similar sentiment was echoed by Christopher Wray, the Director of the FBI, emphasizing the vast scale of cyber threats confronting the U.S., especially those originating from China. The 2023 Annual Threat Assessment by The Office of National Intelligence (ODNI) emphasized the cyber threats posed by China and how it represents the broadest, most active, and most persistent cyber espionage threat to the U.S.

Microsoft, in a report highlighted how a threat actor named Storm-0558 is China-based with espionage related activities. According to the assessment, the modus operandi of the group had some minimal overlap with other Chinese groups such Violet Typhoon (ZIRCONIUM, APT31). The report further detailed that Storm-0558 had mainly targeted diplomatic, economic, and legislative governing bodies in the US and Europe, as well as individuals associated with Taiwan and Uyghur political interests.

Reportedly, other Chinese affiliated groups with similar objectives have also been targeting India's critical infrastructure. According to an assessment, India stands third in Asia-Pacific in terms of cyberespionage attacks on any country in the region. Chinese threat actors have been continuously evolving their tactics to avoid detection. To avoid detection, these actors have employed tactics such as exploiting zero-day vulnerabilities in security, networking and virtualization software. They have also targeted routers and used methods to relay and disguise attacker traffic both outside and inside victim networks. According to Checkpoint, there has been a growing interest among Chinese threat actors in compromising edge devices, with an objective to build resilient and anonymous Command and Control (C&C) infrastructures and to gain a foothold in specific targeted networks.

CRITICAL INFRASTRUCTURE

The year 2023 proved to be challenging for securing critical infrastructure, given the surge in attacks. Over the course of the year, critical infrastructure across the world, including medical, power, communications, waste management, manufacturing, and transportation systems, which serve as vital connections between people and machines, faced almost continual threats. According to an assessment, there were 13 attacks per second, marking a 30% increase from 2022.

Microsoft Threat Intelligence highlighted that in 2023, China affiliated cyber threat actors primarily focused on US critical infrastructure among other sectors. Microsoft also tracked Raspberry Typhoon (RADIUM) as the primary threat group targeting nations surrounding the South China Sea, with a particular emphasis on critical infrastructure, especially in the telecommunications sector. Other sectors targeted include transportation (such as ports and rail), utilities (such as energy and water treatment), and medical infrastructure (including hospitals). According to the Microsoft assessment, this campaign could equip China with capabilities to disrupt critical infrastructure and communications between the United States and Asia.

Reports also emerged of an Iran-linked hacking group actively targeting and compromising multiple U.S. facilities utilizing an Israeli-made computer system. These attacks posed a threat to equipment employed in U.S. water systems and factories. The report indicated that fewer than 10 water facilities were affected by the incident.

The increase in cyber attacks on critical infrastructure was also attributed to the Ukraine-Russia conflict. A Ukrainian hacking group claimed responsibility for an attack on Infotel JSC, a Russian telecom firm crucial to the Russian banking system's infrastructure. The assault on Infotel occurred shortly after a highly anticipated Ukrainian counter-offensive. The Cyber Anarchy Squad, a Ukrainian hacking group active since the onset of the invasion of Ukraine, claimed credit for the attack. The group shared what seemed to be Infotel network diagrams and a screenshot from an Infotel official's email on its Telegram channel.

In a separate yet interconnected event, hackers purportedly targeted Dozor, a satellite telecommunications provider catering to power grids, oil installations, Russian military entities, and the Federal Security Service (FSB). Moreover, the group appeared to disseminate messages supportive of the Wagner group. In December 2023, reports emerged concerning Russian hackers infiltrating the system of the Ukrainian telecommunications giant Kyivstar, with the intrusion dating back to at least May of the previous year. The cyberattack resulted in the destruction of "almost everything," including thousands of virtual servers and PCs. Following the attack on Kyivstar, the Russian Water Utility- Moscow's Rosvodokanal water-management company, fell victim to a retaliatory strike orchestrated by the Ukraine-aligned Blackjack group.

According to reports, Denmark's critical infrastructure faced an intense cyberattack as 22 energy companies fell victim to breaches within a short span of days. In order to maintain an uninterrupted power supply, several of these targeted energy companies were compelled to activate what is known as island mode, disconnecting from the main electric grid and operating autonomously. The identity of the threat actor responsible for the campaign remains unknown, though researchers speculate involvement from multiple groups, potentially including Russia's state-sponsored Sandworm hackers. In a separate incident, Telecommunications Services of Trinidad and Tobago (TSTT) fell prey to a cyberattack resulting in a significant data breach. The ransomware provider RansomEXX claimed responsibility, stating that it had obtained data from a minimum of 800,000 TSTT customers.

INTERNATIONAL DEVELOPMENTS IN CYBER GOVERNANCE

International Cooperation

Member states of the Nordic Council, including Denmark, Finland, Iceland, Norway, and Sweden, had agreed to develop a common cybersecurity strategy. Norway currently holds the 12-month rotating presidency of the Council. While the Nordic Council had been exploring the idea since 2016, the Russia-Ukraine conflict which also resulted in cyber attacks on both Nordic and Baltic states, accelerated the process. Whilst Sweden is investing an additional $130 million in its military budget for 2023-2024 to bolster cyber capabilities, Finland's cybersecurity budget during the same period is being doubled to $80 million. Norway also allocated 21 million euros for cyber defense. The implementing agency, the Nordic Defense Cooperation group, is expected to be tasked with improving intelligence sharing between the militaries and civilian agencies across the Nordic countries.

An international coalition of government cybersecurity organizations published a joint statement and guidance asking software vendors to release future products that are secure by design and secure by default. The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the cybersecurity authorities of Australia, Canada, the United Kingdom, Germany, the Netherlands, and New Zealand in the report titled "Shifting the Balance of Cybersecurity Risks:

Principles and Approaches for Security-by-Design and -Default" urged software manufacturers to take urgent steps to address the issue. The guidance includes specific technical recommendations and core principles to guide software manufacturers in building software security into their design processes before developing, configuring, and shipping their products.

On May 20, 2023, the Quad Leaders' Summit convened in Hiroshima, bringing together Prime Minister Narendra Modi, President Biden of the US, Prime Minister Anthony Albanese of Australia, and Prime Minister Kishida Fumio of Japan. During the meeting, the discussion encompassed various significant initiatives, including critical and emerging technologies. The announcement of "The Quad Partnership for Cable Connectivity and Resilience" signifies recognition of the crucial role played by undersea cables in communication infrastructure. The partnership intends to facilitate access to develop trusted and secure cable systems and establish better internet connectivity and resiliency in the Indo-Pacific.

The Japanese government came out with its plan to build an information network in the Indo-Pacific region to counter cyberattacks with a focus on providing support to Pacific island countries from threat actors. The network will be used for information sharing to provide appropriate time to respond to a cyber incident. The Foreign Ministry had also earmarked strengthening cyber capabilities overseas in the fiscal 2024 draft budget. In addition, Japan plans to build capacity through joint training sessions. Japan is also broadening its cyber capabilities within the Quad framework, comprising the United States, Australia, and India as its members, and through closer collaboration with the Association of Southeast Asian Nations (ASEAN).

During the third International Counter Ransomware Initiative in 2023, members reiterated their shared commitment to enhancing collective resilience against ransomware. This commitment includes collaboration to diminish the viability of ransomware, pursuing those accountable for such attacks, combating illicit finance supporting the ransomware ecosystem, partnering with the private sector to thwart ransomware assaults, and maintaining international cooperation across all facets of the ransomware threat.

Cybersecurity Regulation

Australia unveiled its risk management rules for critical infrastructure and essential services as part of the security measures carried out in accordance with the Security of Critical Infrastructure Act of 2018. The critical infrastructure risk management program provides for annual reporting requirements, compliance and regulatory rules, and mandatory cyber incident reporting, among other measures.

In March 2023, the US administration unveiled its National Cybersecurity Strategy. The Strategy acknowledges that the government must utilize all tools of national power in a coordinated manner to safeguard national security, public safety, and economic prosperity. To realize its vision, the strategy seeks to build and enhance collaboration around five pillars- defend critical infrastructure, disrupt and dismantle threat actors, shape market forces to drive

security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals.

The Austrian Data Protection Authority ruled that Facebook's use of its tracking pixel directly violates the GDPR. Reportedly the personal data was transferred to the US, where the information was at risk from government surveillance. The finding is the result of complaints filed by the European privacy rights group NOYB. However, the data protection authority issued no penalty in the ruling.

The European Parliament's Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware (PEGA) has called on EU officials to create an EU Tech Lab in its final report. The new institution would provide independent research with powers to investigate surveillance, provide legal and technological support, including device screening, and perform forensic research. The final report also condemned the spyware abuses in several EU countries as it pointed out systemic issues in Poland and Hungary. To remedy the situation, the European Parliament members called on the two countries to comply with European Court of Human Rights judgments and restore judicial independence and oversight bodies.

The European Commission announced a new data transfer pact with the United States regarding the transfer of personal data across the Atlantic. According to the new EU-US Data Privacy Framework, the US is expected to ensure adequate protection for personal data transferred from the EU to the US companies. The new framework also introduces new binding safeguards to address all concerns raised by the European Court of Justice, including limiting access to EU data by US intelligence services. It also introduces significant improvements compared to the mechanism that existed under the privacy shield. The efficacy of the framework will be subjected to periodic reviews to be carried out by the European Commission, together with European data protection authorities and relevant US authorities.

For the first time, the lead prosecutor of the International Criminal Court in The Hague had made a clear declaration that the Court will investigate and prosecute cybercrimes that breach established international law, akin to its handling of war crimes occurring in the physical realm. His office will investigate cybercrimes that have the potential to contravene the Rome Statute, which is the treaty that outlines the court's jurisdiction to prosecute unlawful acts, encompassing war crimes, crimes against humanity, and genocide. A spokesperson for the Office of the Prosecutor additionally verified that this is now their official position.

The Australian federal government unveiled the 2023-2030 Australian Cyber Security Strategy, emphasizing the protection of the nation's most vulnerable citizens and businesses. The strategy discusses six overarching shields, namely: Strong businesses and citizens, Safe technology, World-class threat sharing and blocking, Protected critical infrastructure, Sovereign capabilities, and Resilient region and global leadership.

Iran's parliament approved a bill to enhance collaboration with Russia in the field of information security. This development comes as both countries face accusations of conducting extensive cyber attacks. The bill, which enacts an agreement signed three years earlier, has

received approval from Iranian parliamentarians. The bill, containing nine articles, centres on addressing cyber threats, strengthening information security measures, and promoting cooperation between Iran and Russia. A significant aspect of this legislation includes a provision for the exchange of information and collaboration in prosecuting criminal offenses between the two countries.

Discussions on AI

The U.S. President issued an Executive Order focused on Safe, Secure, and Trustworthy AI, with the aim of enabling America to take the lead in harnessing the potential and effectively managing the risks associated with artificial intelligence. The order is aimed at safeguarding American citizens from the potential risks associated with AI. The order establishes new standards for AI safety and security, emphasizing protecting American citizens' privacy. It also highlights concerns about how irresponsible AI usage can exacerbate issues such as discrimination, bias, and other abuses within the realms of justice, healthcare, and housing.

The United Kingdom hosted the first international AI Safety Summit to boost global efforts to cooperate on artificial intelligence (AI) safety. The declaration, by 28 countries and the European Union, was published on the opening day of the AI Safety Summit hosted at Bletchley Park, central England. The summit's agenda centred on identifying mutual AI safety risks, establishing a collective scientific and evidence-based comprehension of these risks, and sustaining the understanding as AI capabilities advance.

The Global Partnership on Artificial Intelligence (GPAI) took place in New Delhi, India. During this meeting, a ministerial declaration was issued, outlining key principles to guide the development of AI. The declaration endorsed the trustworthy and responsible use of AI, reiterating its commitment to a range of broader principles. These principles encompass democratic values and human rights, the safeguarding of dignity and well-being, ensuring the protection of personal data, upholding applicable intellectual property rights, and maintaining privacy and security. Furthermore, the declaration highlights the importance of fostering innovation and advocates for the promotion of AI that is trustworthy, responsible, sustainable, and centered around human needs and values.

MAJOR CYBER INCIDENTS IN THE SOUTH ASIAN REGION

A massive cyber espionage campaign was revealed in the South Asian region in May 2023. In several incidents, hackers sought to exploit fabricated Facebook and Instagram identities to carry out espionage activities, distribute malware, and pilfer information. The hackers posed as journalists, recruiters, military personnel, and others to build trust with their targets. They socially engineered their approach to infiltrate victims' lives. The attacks were launched by multiple advanced persistent threat (APT) groups, some of which appeared to have geopolitical motivations.

INDIA

- Drug major Sun Pharmaceuticals reported that the company faced a cyber-incident perpetrated by a ransomware group. The company reported to have taken appropriate steps to contain the damage and have isolated the impacted assets along with initiating the recovery process. The company also said that business operations have been impacted following the incident and may also have an impact on its revenues.
- Threat actors struck with a series of ransomware attacks across multiple locations in India. In the first incident, over 600 GB of data from Fullerton India, a Non Bank Financial Company (NBFC), was released on the dark web after the company refused to pay the ransom demand of Rs.24 crore. The released data included loan agreements with individuals and legal entities, agreements with banks and other financial institutions, data on international transfers, and personal information of the company's customers such as Aadhaar card numbers, residential addresses, phone numbers, and other sensitive data. In another incident, an Ahmedabad-based hospital was attacked by ransomware actors, demanding USD 70,000 to restore data. The police reported that the hackers demanded the amount through an email and also offered a discount if the hospital agreed to pay the amount.
- Insurance Information Bureau of India (IIB), an independent body, reported that Russian hackers had encrypted their data through a ransomware attack and demanded bitcoins worth $25,000 undo the damage. According to police, some encrypted data included confidential information, and the damage's extent is still being assessed. The police also reported that IIB had a backup of sensitive data, which is helping in continuing daily operations.
- Similarly, a ransomware attack hit Madhya Pradesh Power Management Company Limited (MPPMC) and crippled its internal information technology system used for communication among different functionaries of the state-run entity. The Chief General Manager (IT) of MPPMC said that the attackers had not sought money as yet but had provided email IDs to contact them. Following the complaint, the state cyber cell initiated an investigation into the ransomware attack on the company's IT system.
- In a massive data breach, over 12 thousand confidential records were leaked through Telegram channels, reportedly linked to the SBI account holders and employees. The leaked information included screenshots of the SBI passbook, Aadhaar card, and voter card. The threat actor behind the incident has claimed to have exploited an unprotected database, granting access to the financial details of millions of consumers, like bank balances and recent transactions. The leaked data was also put up for sale in some of the dark web forums by some of these threat actors.

BANGLADESH

- In a massive data leak in Bangladesh, a government website leaked the personal information of citizens, including full names, phone numbers, email addresses, and national ID numbers. According to reports, the leak was accidentally discovered by a

security researcher, following which he contacted the Bangladeshi e-Government Computer Incident Response Team (CIRT). The leak included data of millions of Bangladeshi citizens; however, the name of the website was not revealed to the public.

- There were reports regarding a cyber attack that targeted Bangladesh Airlines, Biman, which resulted in delays in the disbursement of salaries to its employees. According to reports, despite a month and a half passing since the attack, they have failed to fully restore the email server. However, Biman authorities refuted media reports regarding the attack, dismissing them as either baseless or greatly exaggerated.
- During Bangladesh's parliamentary elections, it was discovered that deepfakes had been deployed. Reports indicate that pro-government news outlets and influencers in Bangladesh actively promoted AI-generated disinformation produced using tools provided by artificial intelligence start-ups. In a particular instance, an AI-generated news clip portrayed an anchor criticizing the United States, a nation that the ruling Awami League had strongly criticized in the pre-election period. Another deepfake video, which was subsequently taken down, showed an opposition leader appearing to waver in support of Gazans in the on-going Hamas- Israel conflict. Similar use of deepfakes may be expected in elections in Pakistan and India in 2024.

SRI LANKA

- In September 2023, Sri Lanka experienced a ransomware attack that resulted in the loss of several months' worth of data from thousands of email accounts, including those belonging to high-ranking government officials. Authorities confirmed the occurrence of the attack, which began at the end of August and impacted nearly 5,000 email addresses utilizing the gov.lk email domain. Among the victims were members of Sri Lanka's council of ministers, constituting the central government of the country. The targeted system, Lanka Government Cloud (LGC), along with its backups, was encrypted as part of the attack.

INDIA'S CYBER GOVERNANCE

There were a number of developments on the cyber governance front in India as regulators and relevant ministries brought in policy measures to stem the rising tide of cyber attacks.

The Securities and Exchange Board of India (SEBI) announced a cybersecurity framework for all portfolio managers. The circular asked portfolio managers to report all cyber-attacks and breaches experienced by them within 6 hours of detecting such incidents. The portfolio managers have also been asked to define the responsibilities of its employees, outsourced staff, and employees of vendors and other entities, who may have access to their network. This follows close on the heels of an advisory put out to all regulated entities, including financial sector organizations, stock exchanges, depositories, mutual funds and other financial entities,

in February 2023 asking them to provide compliance of the advisory along with their cybersecurity audit report.

The Insurance Regulatory and Development Authority of India (IRDAI) issued new guidelines on information and cybersecurity for insurers to boost their defences and other institutional arrangements. The guidelines are expected to enable the industry to strengthen its defences and improve its governance mechanisms to deal with emerging cyber threats. The initial guidelines covering information and cybersecurity practices for insurers were issued in 2017. They aimed to ensure that insurers are adequately prepared to manage any cyber threat to their systems. The IRDAI had also established a standing committee dedicated to cyber security. This committee will conduct regular reviews of the risks associated with current and emerging technologies. The committee will also propose suitable modifications to the framework to enhance the cybersecurity readiness and resilience of the insurance industry.

The Indian government blocked 14 mobile messenger applications used by terrorists to receive texts from Pakistan. According to reports, terrorists used these mobile messenger apps to spread and receive messages from Pakistan. The Standing Committee of Finance in the Indian Parliament deliberated on the issue of cybersecurity and rising incidents of cyber/white-collar crimes as lawmakers quizzed experts from the industry about various facets of unlawful activities in cyberspace. The issue of fraud lending apps also came up for discussion at the meeting. Senior officials of different fintech firms and public policy and advocacy groups were among the industry stakeholders who deposed before the committee.

The Reserve Bank of India (RBI) continued with its proactive stance and imposed a penalty of 65 lakh rupees on AP Mahesh Cooperative Urban Bank (APMCUB) for its failure to comply with the Cyber Security Framework for Primary Urban Cooperative Banks. In 2022, hackers breached the security systems of APMCUB and siphoned off 12.48 crore, which the police investigation later revealed, occurred because of the bank's alleged negligence in implementing cybersecurity measures. According to the RBI guidelines, a bank should have security measures like anti-phishing application, intrusion prevention and detection systems, real-time threat defense, and management systems.

On 9 August 2023, the Indian Parliament passed The Digital Personal Data Protection Act to address the issue of personal data and privacy. The law will apply to handling digital personal data in India, whether gathered online or obtained offline and then digitized. It will also apply to data processing activities conducted outside of India if they pertain to offering goods or services within India. Data fiduciaries will be required to preserve data accuracy, security, and deletion upon fulfilling its purpose. The bill also empowers individuals with rights to access information, request corrections and erasure, and seek grievance resolution.

According to reports, future investigations into cyberattacks on India's critical infrastructure and other sensitive digital infrastructure will be led by a specialized anti-cyber terrorism unit (ACTU) created within the National Investigation Agency (NIA). The ACTU, which is yet to be finalized, was sanctioned by the Ministry of Home Affairs in 2022 to investigate the role of terrorists or state actors seeking anonymity.

The Indian Ministry of Defence had decided to transition from Microsoft Windows to 'Maya', an Ubuntu-based operating system developed by Indian government agencies. The Maya OS was developed by Indian government agencies to enhance cybersecurity measures. The new operating system will be supported by a security framework called Chakravyuh. This endpoint security system is concurrently being implemented on computers equipped with the Maya OS.

The Central government has included the Computer Emergency Response Team (CERT-In) in a list of organizations that are exempted from the scope of the Right to Information Act (RTI), 2005.As the national nodal agency for responding to computer security incidents, CERT-In plays a crucial role in addressing such incidents as they arise.

INDIA'S CYBER DIPLOMACY

India was proactive in the cyber diplomacy front throughout the year. The Principal Members of the Quad Senior Cyber Group, including Mr. Michael Pezzullo AO, Secretary of Australia's Department of Home Affairs, Lt. General Rajesh Pant, National Cyber Security Coordinator of India, Mr. Masataka Okano, Deputy National Security Adviser of Japan, and Ms. Anne Neuberger, Deputy National Security Advisor of the USA, convened with their respective inter-agency delegations in New Delhi on January 30-31, 2023. Their primary agenda was to deliberate on a joint strategy aimed at bolstering cybersecurity cooperation and resilience. Following the meeting, the Quad Nations launched a public campaign known as the Quad Cyber Challenge, designed to enhance cybersecurity standards across the Quad nations. Individuals from the Indo-Pacific region and beyond were encouraged to participate in the Challenge and commit to adopting safe and responsible cyber practices.

In the same month, a high level US delegation of the National Science Foundation (NSF) discussed and proposed deeper cooperation with India in areas like Artificial Intelligence (AI), Cyber Security , Quantum, Semiconductor, Clean Energy, Advanced Wireless, Biotechnology, Geosciences, Astrophysics and Defence.

In February under India's G20 presidency, the Secretary of the MeitY inaugurated the G20 Cyber Security Exercise and Drill, which brought together over 400 participants from both domestic and international spheres. The Cyber Security Exercise and drill were conducted by the Indian Computer Emergency Response Team (CERT-In) in a hybrid format, combining both physical and virtual participation. More than 12 countries were represented by international participants who joined remotely via online platforms.

The Second India-Netherlands Cyber Dialogue was held on 3 February 2023 in New Delhi. Discussions at the Dialogue included strategic priorities, cyber threat assessment, next generation telecommunications (including 5G technology) capacity building (including the Indo-Dutch Cyber Security School) and cooperation in multilateral fora, and the latest developments in cyber at the United Nations. The Dialogue was held in the context of recent developments in global cyberspace. It provides both the countries a platform to discuss contemporary topics of importance in cyberspace as well as a range of issues of mutual interest

and facilitates the building of a comprehensive and deeper cyber cooperation between respective cyber agencies/departments in India and the Netherlands.

The Ministry of External Affairs facilitated a virtual meeting between Nigerian and Indian Law Enforcement Agencies (LEAs) on 7 February 2023 to discuss various issues, including WhatsApp impersonation, malware on mobile etc. at the request of I4C, Ministry of Home Affairs. Manager, Nigerian CERT led the Nigerian side during the meeting.

The first experts meeting to negotiate the "draft Statement of Head of State of SCO Member Statement on Digital Transformation" was held online on 20 February 2023. An Indian delegation also participated in the Expert Group Meeting of the Shanghai Cooperation Organisation (SCO) Member States on International Information Security (IIS) was held in Beijing from 15-17 November 2023 in virtual mode. In addition, the National Security Council Secretariat (NSCS) of the Government of India hosted a Practical Seminar on "Countering the Misuse of Internet and New Information Technologies for Terrorist, Separatist, and Extremist Purposes" on December 12, 2023, in New Delhi. The seminar was organized for delegates from the Shanghai Cooperation Organization (SCO) Member States and representatives of the Executive Committee of the Regional Anti-Terrorist Structure (EC RATS) of SCO. This initiative, initiated by India in 2019, falls under the framework of the SCO's Regional Anti-Terrorist Structure (RATS).

In May, as part of India-Israel friendship in the Science and Technology (S&T) both the countries signed a Memorandum of Understanding (MoU) on Industrial Research and Development Cooperation. This milestone agreement was signed between the Council of Scientific and Industrial Research (CSIR) under the Ministry of Science and Technology (MoST) of India and the Directorate of Defense Research and Development (DDR&D) under the Ministry of Defense of the State of Israel.

In June, the 'ARF Workshop on Fostering Professionals in the field of Security of and in the use of ICTs' was held on 13.6.2023 in Hanoi, Vietnam. The second ARF Workshop on "Terminology in the field of Security of and in the use of ICTs in the context of Confidence Building" was also held on 21.6.2023, but in virtual mode.

In the month of July, the Ministry of Home Affairs (MHA) organized a conference on Crime and Security in the Age of NFTs, AI and the Metaverse, in Gurugram, Haryana. Over 900 participants from G20 countries, 9 special invitee countries, international bodies and technology leaders and domain experts from India and across the world attended the two-day conference.

India participated in the Fifth Substantive Session of UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) 2021-2025 which was held at UN Headquarters New York from 24-28 July 2023. Constructive contributions were made to the discussions on various critical aspects of development of rules, norms and principles of responsible behaviour of States in cyberspace, practical confidence building measures and international cooperation in capacity building in the context of existing inequality in cyber preparedness among Member States. A Second

Annual Progress Report was adopted in the Fifth Substantive Session, which marks concrete progress in taking forward the mandate of the OEWG till 2025.

The sixth session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in New York from 21 August to 1 September 2023 in Hybrid mode. MEA representatives provided diplomatic support and outreach to Indian delegation during the sixth session. During the session, the draft text of the convention was also negotiated.

The Fifth edition of the India -Japan Cyber Dialogue was held in Tokyo on 14 September 2023. Led respectively by the Joint Secretary (CD) and Mr Ishizuki Hideo, Ambassador in-charge of Cyber Policy, Ministry of Foreign Affairs (MOFA) of Japan, the two sides discussed areas of bilateral cyber cooperation and exchanged views on latest developments in cyber domain and mutual cooperation at the United Nations and other multilateral and regional fora, including under the Quad framework.

The National Security Council Secretariat coordinated the fourth India-Russia Bilateral Inter-agency consultations on cooperation in ensuring security of the use of Information and Communication technologies (ICT) which was held in New Delhi from 14-15 September 2023.

The Seventh India-EU Cyber Dialogue was held on 05 October 2023 in Brussels. The respective principals from the MEA and the European External Action Service expressed appreciation for the Cyber Dialogue mechanism as it provides a platform to discuss a wide range of issues related to cyberspace. Both sides exchanged views on cyber policies, strategies, and areas of mutual interest. They discussed cyber cooperation in multilateral forums, including at the United Nations, and in regional settings, including at OSCE, ARF, and G20. They also discussed cooperation in promoting capacity building in cyberspace and combating the criminal use of ICTs. Both sides agreed to hold the next India-EU Cyber Dialogue on a mutually convenient date.

India, serving as the Chair of the Global Partnership on Artificial Intelligence (GPAI), successfully hosted the GPAI in New Delhi from December 12 to 14, 2023. The summit featured approximately 30 sessions attended by global AI experts from GPAI, International Organizations, Industry/Startups, and Academia. While some sessions were conducted in closed-door meetings with delegates and GPAI experts, others were held publicly and live streamed for wider participation. The summit attracted over 22,000 attendees, with more than 15,000 AI enthusiasts participating virtually.

The Sixth Substantive Session of the UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) 2021-2025 was held at UN Headquarters New York from 11-15 December 2023. During the session, India made a detailed presentation on the Global Cyber Security Cooperation Portal (GCSCP). The presentation incorporated technical and design details for the proposed portal and also demonstrated how it was more comprehensive as compared to other existing information-sharing platforms.

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