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 2024

AN OVERVIEW OF THE CYBERSECURITY LANDSCAPE IN 2024

The year 2024 presented a fresh array of challenges and opportunities in cyberspace. States undertook significant measures to address and mitigate the existing threats even as new threats emerged. A significant development was the adoption of the United Nations Convention against Cybercrime, a landmark global treaty designed to enhance international cooperation in combating cybercrime and safeguarding societies from digital threats.

This was only a minor triumph when viewed against the escalating wave of cybercrime and the concurrent shortage of cybersecurity experts. The global cybersecurity sector is grappling with a human resource gap, with an estimated shortfall of nearly 4 million professionals worldwide. As demand continues to surge, there is no sign that this challenge will abate in the near future.

A number of reports that came out over the course of the year underscored a concerning surge in cyberattacks amid escalating geopolitical tensions. In November, a Microsoft report outlined an intricate connection between cyber operations and geopolitical conflicts. Similar to the previous year, geopolitical conflicts have extended into cyberspace, with nations increasingly viewing the digital realm as another battlefield. The ongoing Israel-Hamas conflict has also manifested through a surge in cybersecurity attacks. Cyberattacks on critical infrastructure in both Israel and Iran have intensified, with threat actors demonstrating a willingness to cross established red lines. Moreover, there has been a marked rise in influence operations, targeting not only organizations but also individuals on a significant scale. The conflict between Russia and Ukraine also has a significant cyber dimension, with both nations relentlessly targeting each other's state institutions through cyber operations.

State-backed cyber intrusions persisted unabated, further fueled by the global geopolitical instability, with several long-running cyber espionage campaigns coming to light.

Cyber Scam compounds, with operations often linked to human trafficking networks, came to the fore in 2024. Cybercriminals, particularly financial fraudsters, have been using these compounds to conduct their activities globally. A significant portion of these operations originates from Southeast Asian countries, which are increasingly referred to as high-tech fraud hubs. The cybercrime ecosystem is becoming increasingly sophisticated and advanced, employing innovative tactics to deceive and exploit victims.

The ransomware threat continued its relentless advance in 2024, leaving a growing number of victims. Ransomware continues to be the most impactful form of cybercrime worldwide, with numerous organizations reporting significant incidents of ransomware attacks.

In response to these growing threats, international organizations such as INTERPOL have been actively involved in efforts to curb these activities. The United Nations General Assembly adopted the United Nations Convention against Cybercrime, a landmark global treaty designed to enhance international cooperation in combating cybercrime and safeguarding societies from digital threats. Furthermore, an international team of researchers has compiled the first-ever "World Cybercrime Index" The index illustrated that cybercrime, which is often seen as a fluid

and global phenomena, actually has a strong local dimension. The index surveyed five categories of cybercrime, namely: Technical products/services (e.g. Botnet access, access to compromised systems and etc.), attacks and extortion, data/identity theft, scams, and cashing out/money laundering. A key finding was that cybercrime is not universally distributed, but certain countries are turning into cybercrime hubs, in each of the categories.

Cryptocurrency hacking remains a major threat, with over a billion dollars in cryptocurrency stolen in four separate years over the past decade. In 2024, this alarming trend continued, marking the fifth year of such significant thefts. This underscores the direct link between the growing adoption of cryptocurrencies, their increasing market value, and the rising scale of potential thefts.

Threat actors have also been exploiting emerging technologies, such as AI, to carry out stealthy yet sophisticated attacks against their victims. According to reports, AI-driven cyberattacks have emerged as the top risk for enterprises. By leveraging AI, threat actors have been targeting official email addresses, creating vulnerabilities in widely used email services such as Gmail.

As these developments unfold, the year 2025 is expected to bring more significant changes to the cybersecurity threat landscape alongside enhanced regulatory measures by the global community. Forecasts indicate that 2025 will present both challenges and opportunities in the cybersecurity landscape. By 2025, ransomware is expected to become even more sophisticated, with cybercriminals leveraging AI and automation to enhance the speed and precision of their attacks. Overall, the integration of AI into cyberattacks is anticipated to be one of the most significant developments in the cybersecurity landscape. In 2025, organizations will need to prioritize investing in solutions that can effectively vet and monitor their supply chains. Insider threats are also expected to intensify, driven by the continued growth of remote work, AI-powered social engineering, and evolving concerns around data privacy.

ARMED CONFLICTS AND CYBER REALM

In the ongoing Russia-Ukraine conflict, both parties have been relentlessly engaged in cyber warfare against one another. Actors spanning state, state-linked, and non-state entities have been actively involved on both sides of the conflict against each other. Initially, on the defensive, Ukraine has shifted to a more proactive stance in cyberspace as the conflict has progressed. The Ukrainian security and intelligence agencies have begun disclosing some of their cyber operations in Russia against institutions like scientific research centers, state tax service, civil aviation agencies, and its most significant private bank.

Innumerable attacks took place against the systems and infrastructure of both countries. Some of the more prominent attacks are highlighted below. In March, Russia claimed that its systems were being targeted at the time of the presidential election by ‘Western countries’, and also warned of escalating cyber threats from Ukraine.. Hacktivist groups such as Nebula also made concerted attempts to target Russian critical infrastructure and projected its ability to penetrate

secure networks. In April, a Ukrainian hacker group claimed responsibility for a cyber incident targeting the communication system of Moscow's sewage network, preventing the operating company from responding to emergency events. Months later, several Russian banks suffered distributed denial-of-service (DDoS) attacks, severely impacting mobile applications and websites. Similarly, a well-known Russian discount retail chain also suffered a cyberattack that disrupted its services for several days. The incident, reportedly carried out by pro-Ukrainian hackers, targeted the company's website and mobile app, rendering them inaccessible. In a separate incident, several major Russian banks experienced DDoS attacks, causing temporary disruptions to their websites and mobile applications.

Russia has also intensified its attacks on Ukrainian infrastructure, with a particular focus on critical systems and facilities. There were also reports on pro-Russian hackers conducting cyberattacks against South Korea after North Korea sent its troops to support Russian campaign against Ukraine.

Reports also revealed that a Russian military unit was involved in cyberattacks on Ukraine's allies worldwide, aiming to disrupt humanitarian and aid efforts. A pro-Kremlin hacker group claimed responsibility for a coordinated attack targeting the websites of Dutch political parties and EU institutions on the opening day of the European elections. Major tech companies have raised alarms about Russian-linked groups, including hackers associated with Russia's foreign intelligence, attempting to breach their systems using data stolen from corporate emails.

Suspected Russian hackers also carried out one of the largest cyberattacks on Ukraine's state services, targeting state registers that hold critical official records, including biometric data, business and property ownership records, real estate transactions, legal and court decisions, voter information, tax data, and permits. Over time, Russian hacking tactics appear to have evolved. In the first two years of the war, Russian hacker groups conducted opportunistic attacks on a wide range of targets for destructive purposes or cyber espionage. However, this year, their focus has shifted to Ukrainian entities directly tied to the war effort.

The ongoing Israel-Hamas conflict is also unfolding in cyberspace. In early 2024, Rafic Hariri International Airport in Beirut experienced a hacking operation that caused temporary disruption and confusion. Recent reports indicate that shortly before Israel launched its retaliatory attack on Iran, the radar systems within Iran's defense infrastructure were breached, significantly impairing the country's ability to intercept incoming targets. Iranian state agencies and key government branches have also been targeted by threat actors, further escalating cyber tensions.

Hackers infiltrated the system of a Tel Aviv movie theater and screened footage from the events of October 7; an act reportedly carried out by a Turkish threat actor. In a statement, the Israel Defense Forces revealed that its cloud computing network has endured over three billion cyberattacks since the outbreak of the Israel-Hamas conflict on October 7, 2023. However, all attempts were successfully intercepted, preventing any damage. Since the start of the Gaza war, Israel has emerged as the primary target of Iranian cyberattacks, a shift from Tehran's earlier focus on the United States.

MAJOR CYBER BREACHES

Data security remains a critical concern for organizations, not only for ensuring the continuity of business operations but also for safeguarding client privacy. Australian telecommunications provider Tangerine revealed that a cyberattack in February led to the theft of personal information belonging to approximately 230,000 individuals. The attackers gained access to a legacy customer database containing data from both current and former customer accounts.

In March, a significant volume of data from the United Nations Development Programme (UNDP), including information related to staff and internal operations, was stolen and published on a ransomware website. Indian consumer wearable brand boAt experienced a massive data breach, compromising the personal information of over 7.5 million customers. The exposed data included sensitive details such as names, addresses, phone numbers, email addresses, and customer IDs.

In another significant breach, this time targeting military personnel, the names and bank details of thousands of active British soldiers, sailors, and air force members were exposed by a threat actor. AT&T became another victim of a significant data breach, with the call and text records of nearly all its cell customers exposed, impacting millions of users. Star Health Insurance, one of India's leading health insurers, suffered a major data breach, potentially compromising the personal information of 31 million customers. Reports suggest the stolen data has been listed online for sale. Similarly, the Internet Archive's "The Wayback Machine" fell victim to a data breach, with a threat actor compromising the website and stealing a user authentication database containing 31 million unique records.

The cost of such data breaches reached unprecedented levels in 2024, with the global average cost rising to USD 4.88 million- a 10% increase from the previous year and the highest recorded to date.

RANSOMWARE SURGE

Ransomware remains one of the most widespread threats to businesses worldwide, consistently making headlines. These attacks have become increasingly sophisticated and bold, targeting diverse industries and inflicting significant financial, operational, and reputational harm. An analysis of 2024 so far reveals that ransomware groups are not only sustaining their high levels of activity but have further intensified their operations compared to the previous year. Cybercriminals are increasingly focusing on high-value sectors, including critical infrastructure, healthcare, telecommunications, and financial services. Cryptocurrency continues to be the preferred payment method in ransomware attacks, allowing cybercriminals to receive funds anonymously and facilitate cross-border transactions with ease.

This year has also saw significant progress for law enforcement agencies in their operations against ransomware groups. On February 19, 2024, Operation Cronos, a law enforcement initiative, led to outages on LockBit-affiliated platforms, severely disrupting the operations of

the notorious ransomware group. This was soon followed by the UK's National Crime Agency (NCA) taking control of LockBit's leak site, highlighting a unified international effort to combat cybercrime. The months-long operation culminated in the compromise of LockBit's primary platform and other crucial infrastructure supporting their criminal activities. This included the takedown of 34 servers across multiple countries, including the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States, and the United Kingdom. Reports suggest that the ransomware ecosystem is fragmenting due to increasing law enforcement pressure and growing distrust within the cybercriminal community. Although the demise of ransomware has been proclaimed repeatedly in the past, these networks have invariably resurrected after a brief lull, mainly due to the sheer amount of ill-gotten gains available for the taking.

Law enforcement activities saw some notable progress, on the back of broader international cooperation. A global INTERPOL operation, Synergia II dismantled over 22,000 malicious IP addresses and servers linked to cyber threats. The operation, which targeted phishing, ransomware, and information stealers, was a collaborative effort involving INTERPOL, private sector partners, and law enforcement agencies from 95 member countries. Global initiatives, such as the Counter Ransomware Initiative (CRI) during its fourth meeting this year, reaffirmed a joint commitment to enhancing collective resilience against ransomware. The initiative focuses on supporting members facing ransomware attacks, pursuing the perpetrators, denying them safe havens within jurisdictions, countering the use of virtual assets in ransomware operations, collaborating with the private sector to advise and assist CRI members, and fostering international partnerships to combat the growing threat of ransomware better.

AI AND DEEPFAKES

In 2024, AI continued to show immense promise while presenting significant challenges. While 2023 marked the world's discovery of generative AI, 2024 has become the year organizations actively harnessed its potential to generate tangible business value. Surveys reveal a significant surge in AI adoption, particularly within professional services, as organizations increasingly incorporate generative AI into their budgetary planning and strategies. While businesses are reaping the benefits of generative AI, they are also becoming increasingly aware of the diverse risks it poses. These include data management concerns, such as data privacy, bias, and intellectual property (IP) infringement, as well as model management challenges, such as inaccurate outputs and a lack of explainability.

For example, a NIST report titled 'Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations' outlines various adversarial machine learning (AML) tactics and cyberattacks, such as prompt injection, while guiding mitigation and management strategies. NIST identifies two types of prompt injection attacks: direct and indirect. In a direct prompt injection, a user inputs a text prompt designed to manipulate the language model into performing unintended or unauthorized actions. An indirect prompt injection occurs when an

attacker corrupts or degrades the data source that the language model relies on. This highlights the challenges associated with the adoption of generative AI, particularly in ensuring its security and reliability against adversarial threats. Another study reveals that four of the most widely used generative AI chatbots are highly susceptible to basic jailbreak attempts, raising concerns about their security and robustness.

In early 2024, research confirmed that nation-state threat actors are leveraging generative AI tools, including large language models (LLMs) like ChatGPT, to enhance their cyber operations. One of the most widely discussed security risks associated with AI has been the prevalence of deepfakes and their malicious use, particularly in influencing elections, including the U.S. presidential race. Notably, AI played a significant role in the 2024 elections worldwide. Reports also pointed out the spread of misleading narratives in India as well. Big tech giants like Meta have announced the launch of a new helpline and fact-checking service in India, designed to curb the spread of deepfake content on its WhatsApp messaging platform. On the flip side, One of the most impressive and beneficial applications of AI was language translation, with electoral campaigns widely using it to connect with voters across diverse linguistic communities.

The global response to the responsible use of AI has primarily been declaratory, with many countries and organizations emphasizing guidelines and principles without fully implementing enforceable regulations. One significant initiative was the AI Seoul Summit, where participants reaffirmed their commitment to fostering international cooperation and dialogue on artificial intelligence (AI) in light of its rapid advancements and its impact on economies and societies. The participants also acknowledged that AI safety, innovation, and inclusivity are interconnected goals.

The European Parliament has approved the world's first regulatory framework aimed at mitigating the risks associated with artificial intelligence (AI). The AI Act operates by categorizing AI products based on their risk levels and applying corresponding levels of scrutiny. High-risk AI systems, such as those in critical infrastructure, healthcare, and law enforcement, must meet strict regulations. Low-risk services, like spam filters, face minimal oversight, with most AI systems expected to fall into this category.

The White House issued its first-ever National Security Memorandum (NSM) on Artificial Intelligence (AI), emphasizing the significant implications of AI advancements for national security and foreign policy. The NSM directs the U.S. Government to take decisive actions to ensure global leadership in developing safe, secure, and trustworthy AI, harnessing advanced AI technologies to enhance national security, and fostering international consensus and governance on AI.

In 2024, several state governments in India adopted AI-driven initiatives, demonstrating their commitment to utilizing technology to meet regional needs and opportunities. These efforts highlight India's evolution from a passive observer to an active participant in the global AI ecosystem.

EVOLVING CYBERCRIME AND GLOBAL RESPONSE

As previously mentioned, deepfakes have become a significant concern, not only during elections but also in cybercrimes, resulting in millions of dollars in losses for users. At the start of the year, it was reported that a finance employee at a multinational firm was duped into transferring $25 million to fraudsters who used deepfake technology to impersonate the company's chief financial officer during a video conference call.

A sophisticated internet fraud syndicate operating in Zambia was uncovered, resulting in the arrest of 77 individuals, including 22 Chinese nationals. Reports indicated that a Chinese-owned company ran the operation. In a similar operation, Indonesian immigration authorities raided a villa on the resort island of Bali, arresting over a hundred foreign nationals suspected of involvement in cybercrimes. In another law enforcement operation in Africa, eight individuals were arrested as part of an ongoing international crackdown on cybercrime, dealing a significant blow to criminal operations in Côte d'Ivoire and Nigeria. The arrests were made under INTERPOL's Operation Contender 2.0, an initiative designed to combat cyber-enabled crimes, particularly in West Africa, through improved international intelligence sharing. The earlier mentioned Microsoft report reveals the blurring lines between nation-state threat actors and cybercriminals. In 2024, even more state-affiliated actors increasingly adopted criminal tools and tactics and even enlisted criminals to further their objectives.

A study focusing on Southeast Asia reveals that crime syndicates in the region are using malware, generative AI, and deepfakes, along with new underground markets and cryptocurrency, to enhance their operations and facilitate money laundering. Part of their operation involves human trafficking for forced criminality, where organized crime groups compel thousands of workers to scam victims from illegal compounds, often luring them with fake job advertisements.

Cybercrime continues to impose a significant financial toll on the global economy, potentially reaching a staggering $10.5 trillion by 2025. The cost of cybercrime in India has been equally staggering. Estimates suggest that Indian citizens are losing between Rs.1.3 lakh and R.1.5 lakh to cybercriminals every minute.

Numerous cases have been reported in India where scammers are impersonating government officials and law enforcement agencies to defraud victims. The severity of the issue was underscored when Prime Minister Narendra Modi cautioned the public about the growing cyber menace of "digital arrest." In this scheme, fraudsters impersonate law enforcement or government officials to intimidate victims and extort money. In a public advisory, the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs warned internet users about fake emails disguised as government e-notices. These emails, it cautioned, are often scams aimed at defrauding individuals.

The United Nations General Assembly adopted the United Nations Convention against Cybercrime in December 2024. This landmark global treaty aims to enhance international cooperation in combating cybercrime and safeguarding societies from digital threats. The

convention also emphasizes the detrimental effects that cybercrimes can have on states, businesses, and the well-being of individuals and society. It focuses on protecting against offenses such as terrorism, human trafficking, drug smuggling, and online financial crimes.

STATE OF CRYPTOCURRENCY AND REGULATION

Crypto hacking remained a persistent threat in 2024, with stolen funds rising by approximately 21.07% year-over-year (YoY) to $2.2 billion. Additionally, the number of individual hacking incidents increased from 282 in 2023 to 303 in 2024. The shift in focus of threat actors from decentralized finance (DeFi) to centralized services underscores the growing need to secure mechanisms like private keys, which are commonly exploited in hacks.

Central and Southern Asia and Oceania (CSAO) led the Global Crypto Adoption Index 2024, with seven of the top 20 countries hailing from this region. An assessment revealed that Asia leads the world in cryptocurrency adoption, yet regulatory approaches vary widely across countries in the area. Japan has embraced cryptocurrency, recognizing it as both a form of money and legal property. It stands out as one of the few countries globally that have adopted a proactive regulatory framework for cryptocurrencies. The year 2024 marks a pivotal moment for crypto-asset regulation, with countries like Australia, the UK, Brazil, and South Korea announcing plans to introduce new regulatory frameworks.

Indonesian crypto exchange Indodax reportedly faced a security breach, with the company acknowledging a potential issue on the platform. However, it assured users that their balances remained secure, even as trading activities were temporarily suspended. In 2024, India-based cryptocurrency platform WazirX suffered a major security breach, resulting in the theft of cryptocurrency worth at least $230 million.

Reports suggest that India is preparing to regulate cryptocurrency, with the government taking significant steps toward establishing a regulatory framework for the sector. In a notable development within India's cryptocurrency landscape, the Securities and Exchange Board of India (SEBI) has proposed that multiple regulatory bodies be assigned to oversee cryptocurrency trading across the nation.

CYBERATTACKS ON HEALTH SECTOR

This year, the head of the UN World Health Organization (WHO) warned of an alarming surge in ransomware attacks endangering patient safety and destabilizing healthcare systems as the Security Council convened to address the growing threat. Cyberattacks also extended beyond hospitals, disrupting the broader biomedical supply chain. The healthcare industry received mixed news from the Cost of a Data Breach Report 2024. On the positive side, average data breach costs dropped by 10.6% this year. However, for the 14th consecutive year, healthcare recorded the highest breach recovery costs, averaging $9.77 million.

A separate report revealed that ransomware attacks against healthcare organizations have reached a four-year high since 2021. Among surveyed organizations, two-thirds (67%) experienced ransomware attacks in the past year, an increase from 60% in 2023. At a United Nations Security Council briefing in November 2024, U.S. Deputy National Security Advisor for Cyber and Emerging Tech Anne Neuberger specifically called out the role of Russian hackers in perpetuating ransomware attacks against the healthcare sector.

Among the significant breaches in the healthcare sector, a major ransomware attack targeted Romania, taking more than 100 healthcare facilities offline, including at least 25 hospitals. Kuwait's Health Ministry suffered a cyberattack that disrupted systems at several hospitals, also taking down the country's Sahel healthcare app. A ransomware group threatened to publish a large cache of stolen data after attacking a Scottish health board. Authorities later warned that hackers may have accessed "a significant quantity" of patient and staff information. India's healthcare sector continued to be a prime target for cybercriminals, facing over 6,900 cyberattacks every week.

STATE OF EMERGING TECHNOLOGIES

Considering the vast scope and rapid pace of technological advancements across various disciplines, accurately gauging the developments within a single year remains a challenging task. Nevertheless, innovation continues to drive and nurture the growth of emerging technologies. Breakthroughs in AI have positioned it as a transformative general-purpose technology, revolutionizing scientific research. Scientists anticipate that general-purpose AI will revolutionize every aspect of the scientific discovery process in the coming years.

Reconfigurable Intelligent Surfaces (RIS), which leverage metamaterials, smart algorithms, and advanced signal processing to transform ordinary walls and surfaces into intelligent components for wireless communication, are emerging as a groundbreaking technology poised for exponential adoption and growth. Another technological advancement is in the field of High Altitude Platform Stations (HAPS), operating at stratospheric altitudes around 20 kilometers above Earth, offering unparalleled connectivity, coverage, and performance enhancements. They excel in areas with challenging terrains, such as mountains, jungles, or deserts, where satellites and terrestrial towers fall short, making HAPS a pivotal technology for advancing global connectivity.

Other impactful emerging technologies include elastocalorics and carbon-capturing microbes. Elastocaloric heat pumps can significantly reduce energy consumption for heating and cooling, offering a sustainable solution for energy efficiency. Microbial carbon capture is emerging as a promising strategy to control atmospheric CO2 and mitigate global warming.

CYBER ESPIONAGE

In 2024, cyber espionage and surveillance operations were prominent among the cyber operations carried out by both state and non-state actors. Researchers have pointed out a continuing cyber-espionage campaign linked to Russia, targeting human rights organizations, private security firms, and government and educational institutions across Central Asia, East Asia, and Europe using custom malware. These attacks are attributed to a threat actor known as TAG-110, which is likely associated with the Russian cyber-espionage group BlueDelta, also referred to as APT28 or Fancy Bear. Reports highlight a shift in Russia's cyber offensive strategy. Instead of large-scale infrastructure attacks seen in previous years, Russian cyber operatives have now focused on espionage, targeting military and critical infrastructure to support their ongoing war against Ukraine.

An Iranian threat actor reportedly intensified its espionage campaign against Gulf-state government entities, especially in the United Arab Emirates (UAE). The group APT34 (also known as Earth Simnavaz, OilRig, MuddyWater, Crambus, Europium, and Hazel Sandstorm) was linked to the Iranian Ministry of Intelligence and Security (MOIS). APT34 has been known to target high-value sectors across the Middle East, including oil and gas, finance, chemicals, telecommunications, critical infrastructure, and government entities. In their latest attacks, reported in October 2024, APT34 deployed a sophisticated backdoor named Stealthook to exfiltrate sensitive credentials, including accounts and passwords. The attack targeted on-premise Microsoft Exchange servers, using email attachments to transfer the stolen data to servers controlled by the attackers.

Reports also indicated that Belarusian state-sponsored hackers targeted Ukraine's Ministry of Defence and a military base in a new cyber espionage campaign. The attacks were attributed to the Ghostwriter group, a Belarus-linked threat actor known for its previous cyberattacks on Ukraine, Lithuania, Latvia, and Poland. North Korea-linked threat actors have also been actively running cyber espionage campaigns. State-backed hackers from North Korea launched campaigns to steal sensitive information related to nuclear materials, military drones, submarines, and shipbuilding in the UK and the US. Intelligence and security agencies issued alerts and advisories warning of a global cyber-espionage campaign targeting critical industries.

Reports also pointed towards an espionage campaign targeting Indian government agencies and the country's energy sector. The campaign involved a modified version of an open-source information stealer called HackBrowserData, which collects browser login credentials, cookies, and history. According to research, the hackers exfiltrated 8.81 GB of data from their victims, which could potentially facilitate further intrusions into India's government infrastructure.

An espionage campaign with suspected links to Pakistan was uncovered, employing an innovative method to operate malware within compromised Indian government systems. The threat actors, identified as UTA0137, utilized emojis on the Discord messaging platform for command-and-control (C2) communications, effectively evading text-based detection mechanisms.

CHINESE CYBER ESPIONAGE ACTIVITIES

Chinese-linked cyber espionage remained widespread this year, continuing the trend from previous years. The year started with a massive data leak from a Chinese cybersecurity firm, providing a rare insight into the operations of Beijing-linked hackers. The leak exposed a broader campaign aimed at infiltrating critical networks in multiple countries, including India.

A few weeks after the revelation, although unrelated, U.S. and British officials filed charges, imposed sanctions, and accused Beijing of orchestrating a vast cyberespionage campaign. The operation allegedly targeted millions, including lawmakers, academics, journalists, and companies such as defense contractors. The hacking group, which was identified as Advanced Persistent Threat 31 (APT31), is described as an arm of China's Ministry of State Security. The indictment stated that the defendants, along with dozens of identified intelligence officers from China's Ministry of State Security (MSS), contractor hackers, and support personnel, were members of the APT31 group.

According to reports, commercial shipping was among the key targets of a Chinese-linked espionage campaign. The cyber espionage group Mustang Panda deployed malware to gain remote access to the computer systems of cargo shipping companies in Norway, Greece, and the Netherlands. The telecom sector was also among the industries impacted by cyber-espionage campaigns linked to China.

The U.S. government's ongoing investigation into the People's Republic of China (PRC) targeting commercial telecommunications infrastructure uncovered a widespread cyber espionage campaign. Officials stated that the hackers infiltrated the networks of several telecommunications companies to steal customer call records and compromise the communications of a "limited number" of individuals in government and politics. The sophisticated cyberattack, executed by a group of Chinese hackers known as Salt Typhoon, began as early as 2022. U.S. officials stated that its goal was to provide Chinese operatives with persistent access to telecommunications networks across the U.S. by compromising devices such as routers and switches used by companies like AT&T, Verizon, Lumen, and others. There were also reports of a suspected China-based cyber espionage campaign targeting Southeast Asian countries.

Other nations also accused a China-backed group, APT40, of carrying out a large-scale cyber espionage operation. According to the advisory, APT40 is connected to Beijing's MSS. Chinese hackers also breached 20,000 FortiGate systems, a cloud-native firewall used to protect AWS and Azure cloud spaces worldwide. It was alleged that the malware used in the attack could persist in the system even after reboots and firmware upgrades. The attack was believed to have been carried out by a Chinese state-sponsored hacking group as part of a political espionage campaign targeting the Netherlands and its allies.

CRITICAL INFRASTRUCTURE

China and Iran-linked threat actors were reported to be actively targeting critical infrastructure worldwide. At the start of the year, multiple U.S. government agencies reported that China's state-sponsored cyber actors were attempting to infiltrate IT networks to prepare for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States. In a joint advisory, the agencies warned about the Volt Typhoon, which targeted multiple critical infrastructure organizations, focusing primarily on the communications, energy, transportation systems, and water and wastewater systems sectors.

Manufacturing enterprises worldwide were the most targeted, spanning industries such as electronics, automotive, agriculture, medical, and construction. Other sectors, including utilities, transportation, pharmaceuticals, and food and beverage, also faced significant attacks. Geographically, the United States was the hardest hit, accounting for 26% of incidents, followed by Germany (14%) and Australia (9%), with notable cases reported in Colombia, Argentina, and Israel. U.S. utilities experienced a nearly 70% increase in cyberattacks this year compared to the same period in 2023, according to data from Check Point Research, highlighting the growing threat to critical infrastructure. The FBI Director further cautioned national security and intelligence experts about the significant risks China poses to U.S. national and economic security, stressing that critical infrastructure remains a key target.

A report revealed how cyberattacks on power grids, communication systems, transportation networks, ports, and other infrastructure have become "the new geopolitical weapon" in the hands of adversaries, especially the nation-states. For instance, Iranian hackers have reportedly been aggressively attempting to crack passwords in sectors such as healthcare, government, information technology, energy, and engineering.

Iranian cyber actors have also been employing brute force and other techniques to infiltrate organizations across various critical infrastructure sectors, including healthcare and public health (HPH), government, information technology, engineering, and energy. Their likely objective is to acquire credentials and information about the victim's network, which can then be sold to facilitate access for cybercriminals. In response to many such attacks, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) has imposed sanctions on six officials linked to the Iranian intelligence agency for targeting critical infrastructure entities in the U.S. and other countries.

The personal and health data of nearly 13 million Australians were compromised in a cyberattack on medical prescription provider MediSecure. Following an investigation into the dataset accessed by the attackers in May 2024, the company confirmed that 12.9 million individuals who used the MediSecure prescription delivery service between March 2019 and November 2023 were affected. The breach included information related to patient prescriptions.

India has faced a significant amount of cyber attacks on its critical infrastructure in 2024. Threat actors have targeted critical infrastructure sectors such as telecommunications, banking, and

power. In a significant cyber heist, a bank branch in Noida reported a server breach resulting in the illegal transfer of ₹16.50 crore to multiple accounts. A ransomware attack on a technology service provider temporarily disrupted payment systems at nearly 300 small Indian local banks. The attack targeted C-Edge Technologies, a provider of banking technology systems for small banks across the country, reports said. Bharat Sanchar Nigam Limited (BSNL), the state-owned telecommunications provider, experienced a significant data breach in which a threat actor compromised a substantial amount of sensitive data, exposing millions of users to potential risk.

INTERNATIONAL DEVELOPMENTS IN CYBER COOPERATION

International Cooperation

On September 21, 2024, the Quad Leaders' Summit was held, where member countries pledged to create a more resilient, secure, and cooperative cybersecurity environment for the Quad nations and their partners. The Quad countries have been collaborating with software manufacturers, industry trade groups, and research centers to advance their commitment to secure software development standards and certification. Joint efforts are also underway to identify and mitigate vulnerabilities impacting national security and critical infrastructure networks. The Quad is also enhancing coordination on policy responses and sharing cyber threat information regarding significant cybersecurity incidents affecting shared priorities.

As previously discussed, INTERPOL played a crucial role in combating international cybercrime syndicates. However, it was not the only joint law enforcement operation addressing the growing threat of cybercrime. The UK's National Crime Agency (NCA), in collaboration with global partners, including the FBI and agencies from Australia, Canada, and the European Union, launched a series of enforcement actions targeting users of the Cobalt Strike penetration testing tool who were exploiting it for cybercriminal activities. As part of Operation Morpheus, actions were taken last week against 690 instances of Cobalt Strike hosted at 129 internet service providers (ISPs) across nearly 30 countries.

The 68 members of the International Counter Ransomware Initiative (CRI) convened in Washington, D.C., for the Fourth CRI gathering. Members reaffirmed their commitment to strengthening collective resilience against ransomware, supporting affected members, holding perpetrators accountable, preventing safe havens for ransomware actors, countering the use of virtual assets in ransomware schemes, partnering with the private sector for guidance, and building international alliances to more effectively combat ransomware globally. The CRI also released guidance for organizations on handling ransomware incidents. While non-binding and not superseding any specific laws within CRI member jurisdictions, this guidance aims to reduce the overall impact of ransomware attacks on organizations by minimizing disruption and costs to businesses, reducing the number of ransoms paid by victims, and lowering the ransom amounts where victims opt to pay.

Developments in Cyber and Tech Governance Worldwide

President Biden issued an Executive Order with the objective of safeguarding Americans' sensitive personal data from exploitation by countries of concern. The order focuses on protecting Americans' most personal and sensitive information, which encompasses genomic data, biometric data, personal health data, geolocation data, financial data, and certain types of personally identifiable information. In the order, the president directed the Departments of Justice and Homeland Security to collaborate in establishing stringent security standards. These standards are aimed at preventing access by countries of concern to Americans' data through other commercial avenues, such as data accessible via investment, vendor, and employment relationships. President Biden also directed the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, commonly referred to as "Team Telecom," to take into account the threats posed to Americans' sensitive personal data during its reviews of submarine cable licenses.

The Office of the National Cyber Director (ONCD) released the 2024 Report on the Cybersecurity Posture of the United States. The report offers crucial updates on the nation's efforts to tackle the challenges in cyberspace. This report highlights the cybersecurity threats and issues facing the United States, including new and emerging technologies that may impact national security, economic prosperity, and the rule of law. It also includes an assessment of the strategic environment and examines the landscape of emerging technologies and cyber risks, presenting both challenges and opportunities for U.S. cybersecurity policy and strategy. The document also covered the actions taken by the federal government during 2023.

Germany's defense minister unveiled a military restructuring plan in April, which includes the establishment of a new central command and the creation of a dedicated branch for cyberspace. This initiative builds upon the ongoing Bundeswehr overhaul initiated in response to Russia's invasion of Ukraine. The cyberspace branch will specifically target hybrid threats such as disinformation campaigns.

The Royal Thai Armed Forces (RTARF) were directed to establish a Cyber Command Centre by the end of 2024, aiming to increase military capability, enhance cybersecurity, and counter technological threats. The Defence Minister issued the order during a Defence Council meeting in response to concerns over new forms of warfare and global threats, particularly the use of modern technology for attacks or espionage against national security agencies worldwide. The initiative aims to enhance Thailand's cyber capabilities by developing cyber personnel through collaboration with educational institutions, the private sector, and security agencies. The goal is to produce 300-500 skilled personnel annually, as reported.

Prime Minister Fumio Kishida instructed his government to draft potential legislation to introduce an active cyber defense system. This system would enable preemptive actions against cyberattacks, marking a significant step in Japan's cybersecurity strategy. During a meeting, Digital Transformation Minister Taro Kono identified three key issues: strengthening

information sharing between the public and private sectors, identifying servers behind cyberattacks, and determining the extent of authority to be granted to the government.

Indonesian President Joko Widodo and President-elect Prabowo Subianto have approved the creation of a new Cyber Force, which will become the fourth branch of the Indonesian Military (TNI), aimed at enabling the country to "respond effectively to cyberattacks from abroad." The new cyber military unit will operate alongside the Indonesian Army, Navy, and Air Force, and is expected to be a key priority for Mr. Prabowo's incoming Cabinet, according to officials.

Malaysia has launched a Data Breach Notification system designed to ensure prompt reporting and mitigation of data leaks, aiming to protect citizens from becoming victims of fraud, according to Deputy Communications Minister Teo Nie. Data users will now have to report any personal data breaches, including hacking threats. The minister also added that law enforcement agencies, regulatory bodies, and other organizations in Malaysia are collaborating to increase public awareness of the system, enforce stricter regulations, and enhance protection against scams.

Discussions on AI

The European Union Parliament has approved the Artificial Intelligence Act, a legislative measure aimed to safeguard fundamental rights, democracy, the rule of law, and environmental sustainability from the potential risks posed by high-risk AI technologies. The Act also aims to foster innovation and solidify Europe's position as a frontrunner in the AI domain. This regulation imposes obligations on AI systems commensurate with their potential risks and level of impact. The newly implemented regulations prohibit specific AI applications that pose a threat to citizens' rights. These include biometric categorization systems reliant on sensitive characteristics, as well as indiscriminate scraping of facial images from the internet or CCTV footage for the creation of facial recognition databases. Emotion recognition in workplace and educational settings, social scoring, predictive policing solely based on profiling individuals or assessing their characteristics, and AI designed to manipulate human behavior or exploit vulnerabilities will also be banned.

In another significant development, the UN General Assembly unanimously adopted a resolution on Artificial Intelligence. The resolution aims to encourage the protection of personal data, monitor AI for risks, and safeguard human rights. Sponsored by the United States and co-sponsored by 123 countries, it received consensus support from all 193 UN member nations. The resolution also acknowledged the potential of AI systems to expedite and facilitate progress towards achieving the 17 Sustainable Development Goals. This marks the first instance where the Assembly has adopted a resolution on regulating the emerging field.

On July 23, 2024, the competition authorities of the EU, UK, and US issued a joint statement on regulating generative AI. The statement highlighted key concerns, including the concentration of essential AI inputs and potential risks arising from industry partnerships. The statement reaffirmed a shared commitment to ensuring effective competition and the fair

treatment of consumers and businesses. It also emphasized that while their legal powers and jurisdictional contexts differ, all decisions will remain sovereign and independent.

The Cyberspace Administration of China (CAC) released its Guidelines for the Construction of a National AI Industry. The goals include establishing over 50 new national and industry standards by 2026 and at least 20 global standards to advance AI industry development. The Guidelines address key technical standards for AI-related technologies, including machine learning, biometric recognition, and large models.

Hong Kong's government unveiled its first guidelines on the responsible use of artificial intelligence (AI) while also embracing blockchain technology. These efforts aim to position regulators ahead of the technological revolution poised to disrupt financial services.

Singapore introduced new cybersecurity measures to protect AI systems from traditional threats such as supply chain attacks and emerging risks like adversarial machine learning, including data poisoning and evasion attacks. In its Guidelines and Companion Guide for Securing AI Systems, Singapore's Cyber Security Agency (CSA) emphasized that AI systems must adhere to principles of being secure by design and secure by default, akin to other digital systems.

MAJOR CYBER INCIDENTS IN THE SOUTH ASIAN REGION

India accounted for an overwhelming 94.2% of all malware detections in South Asia, underscoring its growing vulnerability in this domain. Furthermore, India led the region in ransomware incidents, with 73.8% of cases, making it a primary target for such attacks. There were some other major attacks on Indian infrastructures across different sectors.

INDIA

- It was reported that in a massive security breach, the System for Pension Administration Raksha (SPARSH) portal, India's central web-based system for automating pension processes for defense personnel, including Army, Navy, Air Force, and civilian defense staff, has experienced a significant data leak.11The data leak of the portal, developed by Tata Consultancy Services (TCS), includes sensitive information such as usernames, passwords, URLs, and pension numbers posing grave threat. to the the privacy and financial security of affected pensioners.
- Personal data belonging to over 7.5 million customers of boAt, a renowned manufacturer of audio products and smartwatches, has surfaced on the dark web, available for purchase at a mere 2 euros. The leaked information includes sensitive personal details such as names, addresses, contact numbers, email IDs, and customer IDs. The breach, totaling approximately 2GB of data, was revealed by a hacker on a prominent forum.

- According to reports, the Tamil Nadu police's Facial Recognition Portal, a software used to track criminals and missing persons, was compromised. Data samples from the portal have been made available for sale on the dark web. An analysis of the leaked samples indicates that 1.2 million lines of data, including names of police officers, phone numbers, and FIR details, have been accessed illegally. A group named 'Valerie' has claimed responsibility for the breach. They have compromised a file containing 55,000 lines of data on police officials, including IPS officers, another file with 890,000 lines of FIR data, and a third file with 2,700 lines of data on police stations (mostly available in the public domain).
- According to reports, there was a breach in the Telangana State (TS) COP app, occurring shortly after reports of the department's HawkEye system being hacked. Data from the Telangana police SMS service portal has reportedly been leaked. Launched in 2018, the app is touted as the first-of-its-kind crime detection tool in India. It features a face recognition system (FRS) to enhance its capabilities in identifying and addressing criminal activities.
- WazirX, a leading Indian cryptocurrency exchange, experienced a major cyberattack in which hackers allegedly stole over $230 million- nearly half of the platform's reserves. This breach underscores the security risks facing cryptocurrency exchanges and their growing appeal as targets for global hackers. In response to the attack, the FBI has contacted Indian cryptocurrency exchange WazirX to investigate the cyberattack, which is reportedly linked to North Korean cybercriminals, and to offer assistance with the probe, according to reports.
- In a major hacking incident, Star Health, one of India's largest health insurance providers, suffered a breach, compromising the personal details of over 31 million customers, including sensitive medical records. The stolen data has been made publicly accessible through chatbots on the Telegram messaging app. Star Health has confirmed the data breach and is working with law enforcement authorities to investigate the incident. Later, Star Health reported receiving a $68,000 ransom demand from a hacker following a breach involving customer data and medical records.

BANGLADESH

- Two senior officials working for the antiterror police in Bangladesh have allegedly collected and sold classified and personal information of citizens to criminals on Telegram, according to reports. The data reportedly sold included national identity details of citizens, cell phone call records, and other classified secret information. These allegations are based on a letter signed by a senior Bangladeshi intelligence official. According to a letter signed by a senior Bangladeshi intelligence official, the police agents were caught after investigators analyzed logs of the National

Telecommunication Monitoring Centre's (NTMC) systems and monitored how frequently the two accessed them.

- The Bangladesh government's initiative of introducing a Cyber Security Ordinance has raised concerns surrounding digital rights and governance. Critics argue that the ordinance is regressive in comparison with other laws pertaining to cybersecurity. The ordinance is structured across nine chapters and 52 sections, covering wide spectrum of preventive measures, crimes and punishments. Also, it mandates establishment of institutions like the National Cyber Security Agency and the National Cyber Security Council.

PAKISTAN

- Pakistan's Permanent Mission to the United Nations was targeted by a cyberattack that has infiltrated its official email account and YouTube channel, according to media reports. The breach targeted the email ID used by the Permanent Mission's information wing. The mission's YouTube channel was compromised, with attackers altering its name, banners, and content. The Pakistani UN mission has requested that all emails and videos posted on its channels be ignored until they regain control of their accounts. No group or entity claimed responsibility for the cyberattack.
- Pakistan's Minister for Information Technology and Telecommunication announced that the government is deploying an internet firewall as part of a cybersecurity upgrade, countering claims that it will suppress free speech. The firewall is part of the country's broader Digital Infrastructure Development Initiative, which has received over $70 million in the latest budget. Critics and digital rights activists express concern that the firewall could be used to stifle dissent, especially as the Pakistani military faces significant online criticism regarding its alleged role in detaining former Prime Minister Imran Khan and cracking down on his party.
- Pakistan's top religious advisory body, the Council of Islamic Ideology, has declared that using virtual private networks (VPNs) to access blocked content is against Shariah law. The ruling comes as the Pakistani government enforces a nationwide firewall and urges users to register VPNs with the state media regulator, citing the need for enhanced cybersecurity and terrorism prevention. However, critics argue that these actions increase online surveillance, restrict freedom of expression, and harm e-commerce. VPNs are commonly used to conceal user identities, ensure privacy, and allow access to restricted content. The council stated that VPNs are being used to access illegal or immoral content, including pornography and disinformation, and emphasized that such actions violate Islamic and social norms.

SRI LANKA

- In January, Sri Lankan lawmakers passed the Online Safety Bill to regulate online content, a move critics argue could suppress free speech. The bill proposes jail terms for content deemed illegal by a five-member commission and holds social media platforms accountable. It was passed with a 46-vote majority in the 225-member parliament, with 108 votes in favor and 62 against.
- Several Sri Lankan government institutions have reportedly been targeted by cyberattacks. Officials confirmed that the official YouTube channel of the Sri Lanka Police Department was hacked. Additionally, the official website of the Sri Lanka Department of Government Printing was compromised, with its data altered. The Sri Lanka Computer Emergency Readiness Team (SLCERT) and the police are jointly investigating the incidents.

NEPAL

- In a breach dating back to 2023, Nepal Rastra Bank was targeted by cybercriminals. The bank took decisive action in February 2024 by filing a claim with the Cyber Bureau to investigate the incident. In March, authorities made an arrest connected to the breach. The breach first came to light in 2023 when a user named "badbuddha" posted on a dark web forum, claiming to possess the source code and sensitive information of Nepal Rastra Bank, Nepal's largest bank, with an asking price of $10,000.

BHUTAN

- The threat actor Patchwork has been implicated in a cyberattack targeting entities connected to Bhutan, deploying the Brute Ratel C4 framework and an updated variant of the PGoShell backdoor.Active since at least 2009, Patchwork is known for spear-phishing and watering hole attacks, particularly against targets in China and Pakistan, as reported by Chinese cybersecurity firm QiAnXin.

INDIA'S CYBER GOVERNANCE

Significant steps were taken by the government, including initiatives at the state level, to address cybersecurity challenges and enhance digital resilience.

- In response to the increasing number of cyber incidents, particularly financial fraud, the Secretary of the Department of Financial Services (DFS) under the Ministry of Finance chaired a meeting to address pressing concerns regarding cybersecurity in the financial services sector and to devise comprehensive strategies to mitigate such threats. One of

the key highlights of the meeting was the action taken by the Department of Telecom in blocking approximately 1.4 lakh mobile handsets associated with financial fraud.

- In a proactive step to enhance the cyber defense capabilities of the Indian Armed Forces, the Defence Cyber Agency (DCyA) conducted the Chief Information Security Officers (CISO) Conclave – 24. This two-day event, which took place on March 14th and 15th, 2024, gathered officers from the tri-services of the Indian Armed Forces under the oversight of Headquarters Integrated Defence Staff (HQ_IDS). A notable feature of the event was the execution of situation-based Table Top Exercises (TTX) designed to practice incident response protocols. These exercises, facilitated by the Data Security Council of India (DSCI), replicated genuine cyber threats and scenarios, allowing participants to evaluate their readiness and collaboration in effectively managing cyber incidents.
  According to reports, the Indian Army has established an elite unit called the Signals Technology Evaluation and Adaptation Group (STEAG), tasked with researching and evaluating futuristic communication technologies such as 6G, Artificial Intelligence (AI), Machine Learning (ML), and quantum computing for military applications, given the evolving nature of the field. Officials stated that STEAG is entrusted with fostering technologies encompassing the entire spectrum of wired and wireless systems. The creation of STEAG is a strategic move by the Army to develop technologies in anticipation of future battlefield requirements.

- The Computer Emergency Response Team (CERT-In) is collaborating with Mastercard to enhance cooperation and information sharing in cybersecurity within the financial sector. Under a Memorandum of Understanding (MoU), the two organizations will leverage their expertise to focus on cybersecurity incident response, capacity building, and sharing cyber threat intelligence specific to the financial sector. This partnership also includes advanced malware analysis initiatives.

- The Reserve Bank of India (RBI) has proposed the establishment of a Digital Payments Intelligence Platform aimed at leveraging advanced technologies to mitigate payment fraud risks. To advance this initiative, the RBI has formed a committee chaired by A.P. Hota, former MD & CEO of NPCI. The committee's mandate is to assess various aspects related to setting up a digital public infrastructure for the platform. The committee is expected to deliver recommendations within two months.

- To address the growing issue of spam calls affecting Indian consumers, the Telecom Regulatory Authority of India (TRAI) mandated an immediate halt to all voice promotional calls from unregistered senders or telemarketers. Announced in August, this directive seeks to provide much needed relief to mobile phone users nationwide. The directive requires all access service providers, including telecom operators, to immediately cease facilitating pre-recorded or computer-generated promotional voice calls from unregistered sources.

- The Karnataka government has unveiled its Cybersecurity Policy 2024, allocating Rs 104 crore to tackle online crime and enhance cybersecurity awareness over the next five years. The policy, which is divided into two parts, aims to bolster cybersecurity across various sectors- including the public, academia, industry, startups, and government- and improve the state's IT infrastructure. Key focus areas of the awareness program include education, skill-building, industry and startup promotion, and capacity-building partnerships.

- The Union Ministry of Electronics and Information Technology (MeitY) plans to assign trained data experts and analysts to various central government ministries and departments, according to reports. These specialized analysts will focus on streamlining the internal datasets managed by different ministries, improving data handling and analysis across the government.

- The government has partnered with IITs and IIITs to train the first batch of cyber commandos, with the special unit set to be commissioned in the coming months. Nearly 350 personnel, selected from various state police forces, will be trained to handle and counter cyberattacks. The training program includes investigation officers and senior police officers, who will be equipped to respond to and manage cyber threats, officials noted.

- The Tamil Nadu government recently unveiled its Cyber Security Policy 2.0, outlining measures to safeguard government assets. The policy includes guidelines and Standard Operating Procedures (SOPs) for auditing, compliance, and monitoring cyber threats and attacks. The Cyber Security Policy 2.0, issued on August 23 this year, is set to replace the Tamil Nadu Cyber Security Policy 2020, which was introduced in September 2020. The updated policy includes contributions from the Centre for Development of Advanced Computing (C-DAC), the Indian Institute of Technology Madras (IIT-M), and the Tamil Nadu e-Governance Agency, among others.

- The Minister of Home Affairs has launched an online 'suspect registry' containing data on 1.4 million cybercriminals involved in financial fraud and various cybercrimes. Developed by the Indian Cyber Crime Coordination Centre (I4C), the registry is accessible to states, Union Territories, and central investigation and intelligence agencies. The collaboration with banks and financial intermediaries aims to strengthen fraud risk management within the country's financial system.

- The government has designated the National Security Council Secretariat (NSCS) as the nodal agency for addressing the rising cyber security threats. According to the notification, specific responsibilities have been assigned to various ministries for enhanced clarity. The telecom department will oversee telecom network security, the IT department will handle cyber security, and the home ministry will focus on combating cybercrime.

- The Bengaluru Metro Rail Corporation Limited (BMRCL) is set to establish a dedicated Security Operations Centre (SOC) to counter cyber threats, becoming the first metro operator in India to do so. The SOC aims to enhance preparedness against potential cyberattacks, leveraging AI and machine learning to tackle automated threats. According to a senior BMRCL official, it will provide comprehensive network visibility by collecting logs from all devices.
- The Telecom Cyber Security Rules, 2024, enforced by the Department of Telecommunications in November, require telecom entities to report cybersecurity incidents to the central government within six hours of detection. This aligns with the six-hour timeline specified in the 2022 CERT-In directions. Entities must also provide details of the affected system and a description of the incident within this period. Released for public consultation on August 29, the rules mandate telecom operators to adopt measures to prevent and address cyber threats.

INDIA'S CYBER DIPLOMACY

- The Indian delegation actively participated in the deliberations of the UN Ad Hoc Committee to elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes
- An Indian delegation also participated in the 12th ASEAN Regional Forum (ARF) Open-Ended Study Group (OESG) on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the use of Information and Communications Technologies in the field of Security of and in the use of ICTs' was held on February 26 2024.
  The Indian government announced the rescue of 250 citizens from Cambodia, where job opportunities lured them but ultimately coerced them into perpetrating cyber fraud. In response to media queries, the spokesperson for the Indian Ministry of External Affairs said that the Indian Embassy in Cambodia is actively responding to complaints from Indian nationals who were forced to do illegal cyberwork.
- The Sixth Cyber Dialogue between India and the United Kingdom took place on July 3, 2024, in New Delhi. The discussions covered topics such as cyber threat assessment, internet governance, data protection, critical infrastructure protection, capacity building, and cooperation in multilateral forums, including recent developments in the cyber realm at the United Nations. Both nations agreed to enhance cooperation between their cyber agencies to ensure a safe and robust cyberspace.
- The 6th meeting of the GPAI Ministerial Council took place on July 3, 2024, at Bharat Mandapam, New Delhi, in a hybrid format. After extensive discussions, members reached a consensus on the future vision of the Global Partnership on Artificial Intelligence (GPAI). They recognized the transformative potential of AI in shaping

societies and economies while also acknowledging the emerging risks and challenges posed by AI systems, among other key considerations.

- The Central Bureau of Investigation (CBI) arrested 26 individuals in Pune, Hyderabad, and Visakhapatnam as part of a major operation against a tech-enabled crime syndicate. The crackdown spanned 32 locations and uncovered a network that targeted victims overseas. In the process, the CBI identified 170 suspects believed to be involved in illegal online activities through four call centers. The investigation into the cybercrime network is being carried out in close coordination with the United States Homeland Security Investigations and other international law enforcement agencies.
- The inaugural ASEAN-India Track 1 Cyber Policy Dialogue took place on October 16, 2024, in Singapore. It was co-chaired by Mr. Amit A. Shukla, Joint Secretary of the Cyber Diplomacy Division, Ministry of External Affairs, and Mr. Jeffrey Ian Dy, Undersecretary for Infrastructure Management, Cybersecurity, and Upskilling from the Philippines. During the dialogue, participants shared insights on the cyber threat landscape, national cybersecurity policies, threat assessments, and recent ICT developments at the United Nations. They also discussed cooperation in capacity building and training to pinpoint specific areas for collaborative action.
- India and Singapore held their first Cyber Policy Dialogue on October 17, 2024, in Singapore, co-chaired by Mr. Amit A. Shukla and Mr. David Koh, Chief Executive of Singapore's Cyber Security Agency. The dialogue covered the cyber threat landscape, national cybersecurity strategies, and global cyber governance developments under the UN. They also explored bilateral cooperation in cyber threat response, critical infrastructure protection, and joint capacity-building initiatives.
- During the first India-Italy Bilateral Cyber Dialogue, both sides shared perspectives on the cyber threat landscape and national cybersecurity strategies. They discussed critical infrastructure protection, capacity building initiatives, and collaboration in multilateral forums, particularly on recent UN developments in cybersecurity. Both countries agreed to strengthen cooperation between their agencies to promote a safe and resilient cyberspace.

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