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

CyberSecurity
Centre of Excellence

Major Events and Trends in Cybersecurity in 2025

An Overview of the Cybersecurity Landscape in 2025

The year 2025 was characterised by a persistent surge in cybersecurity incidents, with reports emerging almost on a weekly basis illustrating how digital vulnerabilities have become deeply and continuously integrated into the global security environment; rather than being confined to isolated moments, these incidents underscored how deeply and continuously digital vulnerabilities shaped the security environment throughout the year. As in previous years Ransomware continued to be a systemic risk capable of crippling national supply chains and critical industries like healthcare, energy, and finance. The year was further characterised by the transformative impact of artificial intelligence (AI), which shifted the advantage toward threat actors through sophisticated phishing and deepfakes, and the increasing spillover of armed conflicts into the cyber domain. Despite these challenges, 2025 also saw landmark achievements in international cooperation, including a historic UN cybercrime treaty and coordinated global law enforcement actions that successfully dismantled major criminal infrastructures.

Highlights of the Year

In an unprecedented development, members of the UN Security Council convened for the first time to discuss the threat posed by commercial spyware during an informal meeting. This Arria-formula meeting, which typically involves deliberation on pressing issues outside the Council's formal agenda, was held amid growing concern over the use of spyware to infiltrate the devices of diplomats and other officials.

At the beginning of the year, privacy and security concerns emerged around DeepSeek, a Chinese AI startup that drew global attention following the release of its DeepSeek R1 model. The company claimed that the model rivalled the capabilities of technologies developed by OpenAI, while being significantly cheaper to develop. Following the release of its R1 model, debates over restricting or banning DeepSeek gained momentum, particularly within government offices in countries that raised concerns about the application's security and data practices.

The year also witnessed a surge in cyberattacks targeting the aviation sector, as attackers recognised that even short-lived disruptions can have wide-ranging financial, operational, and reputational consequences. In the same vein, the healthcare sector was not spared from cyber incidents, making 2025 yet another difficult year marked by persistent and damaging healthcare data breaches.

The steady rise in ransomware attacks in 2025 indicated that the threat had not merely expanded in scale but had evolved in nature. During the year, the ransomware landscape shifted in ways that went beyond routine patterns. No longer limited to isolated IT incidents, ransomware emerged as a systemic risk capable of disrupting national supply chains, critical services, and entire industries. Global ransomware attacks targeting critical industries rose by 34 % in 2025. Nearly half of these incidents struck sectors central to national resilience, including manufacturing, healthcare, energy, transportation, and finance. Together, these trends highlight why ransomware continues to pose a serious and persistent threat to national security.

Cryptocurrency theft intensified in 2025, with total losses exceeding $3.4 billion despite a decline in the number of large-scale incidents. North Korea remained the most prominent threat actor, responsible for stealing at least $2.02 billion in digital assets during the year, amounting to a 51 per cent increase compared with 2024.

Continuing the broader pattern, armed conflicts increasingly spilt over into the cyber domain. As the Russia-Ukraine conflict persisted in cyberspace, the Israel–Iran military confrontation also produced clear cyber repercussions, underscoring how contemporary conflicts now unfold simultaneously across physical and digital fronts. Nation-state cyber threats continued to persist across the globe, with state actors targeting key industries and regions primarily for espionage, and in some cases for financial gain.

China expanded its cyber operations against a wide range of industries and non-governmental organisations, often exploiting vulnerable devices to maintain covert access. Iran focused on logistics companies in Europe and the Persian Gulf, suggesting preparations to disrupt commercial shipping and trade routes. Russia extended its cyber activities beyond Ukraine, increasingly targeting small businesses in NATO countries and using them as gateways into larger organisations. North Korea remained heavily focused on financial theft and espionage, including the use of overseas IT workers whose earnings were funnelled back to the regime.

The growing prevalence of cyber scam compounds and organised fraud centres was another defining phenomenon that marked 2025. Across Southeast Asia, an expanding network of transnational criminal operations affected tens of thousands of lives. In response, law enforcement agencies stepped up coordinated action against these organised malicious actors, and INTERPOL's General Assembly adopted a resolution to address the growing threat posed by transnational scam centres and criminal hubs linked to large-scale fraud, human trafficking, and abuse.

The sustained use of AI for malicious purposes further shifted the cyber threat landscape in favour of threat actors. Attackers increasingly leveraged AI to generate highly realistic phishing campaigns at scale, clone executive voices, probe exposed AI infrastructure, and automate key stages of cyber intrusions. Cybercriminals increasingly exploit AI to carry out more sophisticated and rapid attacks, automating phishing campaigns, producing convincing deepfakes, and probing systems at a swift speed. Reflecting the scale of this shift, a 2025 study found that 87 per cent of organisations reported experiencing at least one AI-driven cyberattack over the past year.

The year 2026 is poised to bring a mix of significant opportunities alongside complex and evolving challenges. Agentic AI, for instance, is set to become a double-edged sword, as it is likely to be deployed by both attackers and defenders in the evolving cyber landscape. Autonomous AI agents are rapidly reshaping enterprise risk, placing a growing strain on legacy security models that are increasingly ill-equipped to withstand this pressure. At the same time, AI is exposing organisations to unprecedented risks of intellectual property loss. Assessments suggest that 2026 is likely to witness major security incidents in which sensitive IP is compromised through the use of shadow AI systems, such as unapproved tools deployed by employees without adequate oversight.

At the same time, the rapid advancement of quantum computing is prompting an urgent need to develop and implement plans for upgrading existing cryptographic systems. With quantum computing approaching reality, the push to adopt quantum-safe algorithms adds yet another layer of complexity. Organisations that are slow to adapt may find themselves increasingly exposed, struggling to evolve quickly enough to keep up with a rapidly changing threat environment. As the world transitions into 2026, the focus must pivot toward managing the "double-edged sword" of agentic AI and accelerating the transition to quantum-safe cryptography to maintain digital sovereignty in an increasingly complex threat environment.

ARMED CONFLICTS AND CYBER REALM

Both Russia and Ukraine continued to carry out cyber operations against one another as part of the ongoing conflict. In January 2025, Ukraine restored its state registry infrastructure after it was disrupted by a major cyberattack believed to have been carried out by hackers linked to Russia's military intelligence. The attack temporarily prevented citizens from accessing essential public services connected to their digital records. In March, Ukrainian Railways was targeted by a large-scale and sophisticated cyberattack. However, reports indicated that the attackers were unable to disrupt operations, and railway traffic continued to run without delays.

Russia also reportedly stepped up its use of artificial intelligence to analyse data stolen through cyberattacks, enhancing the precision and effectiveness of its operations, particularly for cyber espionage purposes. In fact, these attacks were not confined to Ukraine, with several instances of more widespread cyber operations also reported across Europe. For instance, the French Foreign Ministry attributed a series of cyberattacks targeting French national interests to APT28, a threat group linked to GRU, and strongly condemned the Russian state's use of such cyber operations. Some threat assessments suggested that Russia increased its cyberattacks against NATO member states by around 25% compared to previous year. Reports also indicated that nine of the ten countries most affected by Russian state-linked cyber activity belonged to the NATO alliance.

Drawing on its experience from the ongoing war and the reality of cyber warfare, the Ukrainian Parliament has recently backed, at the first reading, the creation of dedicated Cyber Forces within Ukraine's military, further highlighting the growing strategic importance of cyberspace in the conflict with Russia. The bill, supported by 255 lawmakers, seeks to establish the Cyber Forces as a formal military command responsible for strengthening Ukraine's defence and security capabilities in the cyber domain.

Ukraine also demonstrated its offensive cyber capabilities throughout the year, carrying out operations that targeted Russian systems and interests in cyberspace. In March 2025, a Ukrainian volunteer hacker collective known as the IT Army of Ukraine claimed responsibility for a cyberattack against a Russian internet service provider. The attack reportedly disrupted services in Moscow and St. Petersburg for three days. Beyond telecommunications networks, Ukraine's military intelligence agency, also known as HUR, targeted Russian government systems. In one such operation, HUR reportedly hacked the Central Election Commission of Russia and other state services in response to voting processes conducted in territories that Ukraine considers to be under Russian occupation.

The Russian aviation company Aeroflot was forced to cancel dozens of flights after a pro-Ukraine hacking group claimed responsibility for a cyberattack. In response, the Kremlin described the situation as concerning and confirmed that the airline's disruptions were caused by a cyber incident.

A similar pattern of cyber operations unfolding alongside kinetic hostilities was also evident during the brief 12-day conflict between Israel and Iran, highlighting how cyber activity has become an integral feature of modern armed confrontations. Shortly after news of the military operation broke, Iran-aligned threat actors ramped up activities on their public and private Telegram channels. The Cyber Bulletin channel received a message from an actor under the alias #OpIsrael, claiming attacks on Israel's Tzofar public alert system, which warns civilians of missile threats. Meanwhile, groups like Mysterious Team Bangladesh warned Jordan and Saudi Arabia of potential cyberattacks on their national infrastructure if they support Israel.

On the other side, pro-Israel hacking group Predatory Sparrow, reportedly linked to Israel, claimed a cyberattack on an Iranian bank in retaliation for its alleged role in funding Iran's military and nuclear programs. Iran's state-owned TV broadcaster was also hacked overnight, disrupting regular programming to air videos urging street protests against the Iranian government, according to multiple reports. The identity of the attackers remains unknown, though Iranian authorities had accused Israel of being behind the incident. Reports also indicated that Iran has been tapping into private security cameras in Israel to gather real-time intelligence, highlighting a recurring vulnerability in such devices that has surfaced in other global conflicts as well.

The armed conflict between India and Pakistan was also accompanied by sporadic cyber incidents. A wide range of actors were active on the cyber front, including loosely organised hacktivist collectives, individual patriotic hackers, and, in some cases, operators with possible links to state institutions. Cyber operations during the conflict were marked more by their public signalling than by deep technical sophistication. Roughly half of the documented incidents consisted of distributed denial-of-service (DDoS) attacks designed to take websites offline, while around one-third involved website defacements. A smaller number of cases included alleged data breaches, which were generally limited in scope as well as attempted network intrusions.

Major Data Breaches

The year 2025 offered little respite from data breaches, with reports of such incidents emerging consistently throughout the year and across regions worldwide. In January, the International Civil Aviation Organization (ICAO) confirmed a cyberattack on its recruitment systems that led to the compromise of personal data. The incident involved the exposure of more than 40,000 records, with the threat actor claiming to have released approximately 42,000 recruitment application files dating from April 2016 to July 2024.

In a separate incident, the United States Coast Guard took its personnel and payroll system offline following a data breach that affected more than 1,100 service members. The Coast Guard confirmed that its Direct Access system, which manages pay and personnel functions, including official orders, had been compromised, exposing sensitive data such as bank routing numbers and direct deposit account information.

A hacker reportedly compromised the GitLab repositories of Europcar Mobility Group, stealing source code for the company's Android and iOS applications along with personal data belonging to up to 200,000 customers. The attacker subsequently attempted to extort the company by threatening to release around 37 GB of stolen data, reportedly including system backups and sensitive information related to Europcar's cloud infrastructure and internal applications.

Later in the year, the House of Commons of Canada disclosed a data breach resulting from the actions of a threat actor who targeted employee information. Parliamentary authorities informed staff that a malicious actor had exploited a recently identified vulnerability in Microsoft software to gain unauthorised access to a database used for managing government-issued computers and mobile devices.

Automotive manufacturing giant Stellantis also confirmed that attackers had stolen data belonging to some of its North American customers after gaining access to a third-party service provider's platform. According to reports, the breach was limited to customer contact information, as the compromised system did not store financial details or other highly sensitive personal data.

Panama's Ministry of Economy and Finance (MEF) also announced that threat actors compromised one of its computers. In its statement, MEF said it detected signs of possible malicious software on a workstation and responded swiftly by isolating the affected system, thereby preventing the threat from spreading across the wider network.

In December 2025, Nissan disclosed that thousands of its customers had been affected by a data breach following unauthorised access to a server managed by Red Hat. The incident impacted approximately 21,000 customers.

Recurrent Ransomware

The Qilin ransomware-as-a-service group claimed responsibility for hacking the Palau Ministry of Health and Human Services (MHHS) in a leak post in February 2025. Palau officials later confirmed that the ransomware attack, carried out by hackers linked to the group, enabled the attackers to steal files from IT systems used by the MHHS. It was also later confirmed that government officials contained the incident and restored hospital operations to normal within 48 hours with assistance from Palauan and Australian cybersecurity experts, along with officials from the Ministry of Finance.

In another incident, Kidney dialysis provider DaVita disclosed that a ransomware attack disrupted parts of its operations, encrypting sections of its network. In a filing with the U.S. Securities and Exchange Commission, the company stated it had activated its response protocols, isolated affected systems, and implemented containment measures. DaVita promptly implemented containment measures and isolated the affected systems following the ransomware attack. The company also enlisted third-party cybersecurity experts and notified law enforcement to assist in the investigation and response.

It was also reported that a ransomware attack on Miljödata, a Swedish software provider, affected around 200 municipal governments across the country. According to reports, the attackers are attempting to extort the company. Reports also indicate that Miljödata worked jointly with external experts to investigate the incident and determine the scope of impact and those directly affected.

On September 16, Jaguar Land Rover (JLR) confirmed a cyber incident. Although not officially confirmed, the incident was widely linked to earlier attacks in which the HELLCAT ransomware group had reportedly targeted Jaguar Land Rover, exfiltrating hundreds of internal documents and compromising employee data through the misuse of stolen Jira credentials.

In November, Japanese beverage giant Asahi disclosed that a major cyberattack earlier in the year may have led to the exposure of personal data belonging to more than 1.5 million customers. In a statement outlining the findings of its investigation, the company said the ransomware attack had severely disrupted operations across its factories in Japan, forcing employees to revert to manual, pen-and-paper processes to manage orders. Asahi further noted that personal information of individuals who had contacted its customer service centres was likely compromised in the attack.

Asustek Computer Inc., a major Taiwanese electronics company, confirmed that one of its suppliers was hacked, leading to the exposure of image-processing source code used in some of its mobile phone cameras. While the company did not identify the attacker, the disclosure followed earlier reports that the Everest gang claimed to have breached Asus and stolen more than 1 terabyte of data, including camera source code. The company declined to validate Everest's broader claims, saying the breach was limited to an unnamed supplier whose systems hosted camera-related code, and has not clarified whether the data involved was proprietary Asus material or belonged to other firms cited by the group.

According to an annually published ransomware assessment, enterprises identified exploited vulnerabilities as the most common technical root cause of attacks, accounting for 29% of incidents. Phishing and compromised credentials followed, each cited in 21% of cases. It was also noted that, beyond technical weaknesses, several operational factors also contributed to organisations falling victim to ransomware, with no single issue emerging as the dominant cause.

In a concerning trend, nearly half of enterprise organisations (48%) paid ransoms in 2025 to recover their data, broadly in line with levels observed over the past four years, suggesting little change in payment behaviour. At the same time, reliance on backups fell to a four-year low, with only 53% of organisations using them for recovery, down sharply from 73% the previous year.

When Hackers become the Victim

In an interesting turn of events, 2025 was not an easy year for malicious threat actors either, as several of them themselves became victims of data breaches and cyber intrusions. The ransom-seeking cybercriminal group LockBit was hacked, with leaked data reportedly including chat logs between the hackers and their victims. The group's dark web affiliate panels were defaced and replaced with a message linking to a MySQL database dump.

In another reported incident, a major data leak compromised the Chinese security firm Knownsec, exposing more than 12,000 confidential files on GitHub and offering rare insights into China's state-linked hacking tools and operations. Knownsec, a well-known actor in China's cybersecurity ecosystem, was reportedly involved in developing the so-called cyber weapons and maintaining lists of international targets. The leaked material pointed to extensive surveillance activities spanning more than 20 countries, including operations directed at critical infrastructure entities such as telecommunications companies.

Later in the year, a threat intelligence firm examined a dataset believed to be a credible leak of operational materials linked to Charming Kitten (APT35). The material included Persian-language internal documents, personnel lists, details of custom tools, and campaign reports. Together, these records outlined a highly structured operation, with dedicated teams responsible for network penetration, malware development, social engineering, and infrastructure compromise. Overall, the disclosure underscored Iran's well-organised regional espionage capabilities and highlighted the serious supply-chain and national security risks posed by Islamic Revolutionary Guard Corps (IRGC)-affiliated cyber actors.

AI-Powered Cybersecurity Issues

In 2025, AI-powered cyberattacks were reportedly more sophisticated and adaptive, demonstrating a higher degree of precision than in previous years. For example, Sony highlighted the mounting challenges confronting the music industry, drawing attention to the growing economic cost of unauthorised AI-generated reproductions. In its submission, Sony stated that it had already issued more than 75,000 takedown requests for AI-generated content impersonating some of its most prominent artists.

In another incident, the US Department of State confirmed that it was investigating an imposter who used AI to impersonate Secretary of State Marco Rubio and make contact with three foreign ministers. While serious, the episode was not unprecedented, as AI-enabled impersonation has previously been used to mimic senior US political figures.

According to an annual threat assessment, unmanaged use of generative AI is driving widespread data exposure across enterprises. It also noted that as organisations move into 2026, there is a growing need to prioritise prevention-first security approaches, invest in real-time AI threat intelligence, and establish strong governance frameworks to control how AI tools are deployed and used across the business. Another concern highlighted was that, beyond vulnerabilities in the tools themselves, research showed that one in every 27 generative AI prompts submitted from enterprise networks carried a high risk of sensitive data leakage. The report further noted that an overwhelming majority of organisations using generative AI tools 91% were affected by such high-risk prompt activity.

Threat actors are increasingly embedding AI into their operations to amplify the scale, speed, and sophistication of attacks, particularly in areas such as AI-powered phishing and social engineering. Modern large language models (LLMs) can analyse a target's public digital footprint, ranging from social media activity and professional profiles to company announcements, to tailor highly personalised and convincing narratives that exploit human trust. This threat is further intensified by the growing accessibility of advanced attack tools.

CYBER ATTACKS AGAINST SPACE AND AVIATION ASSETS

The year 2025 stood out for a marked rise in cyberattacks targeting space and aviation assets, including national and regional space agencies as well as airport infrastructure. In March, Polish cybersecurity services detected unauthorised access to the IT infrastructure of the Polish Space Agency (POLSA), an incident that was subsequently confirmed by the relevant authorities. The agency acknowledged that it had experienced a cybersecurity breach and, as a precautionary measure to limit potential repercussions, disconnected its network from the internet.

More recently, European Space Agency (ESA) issued a brief statement appearing to confirm reports that hackers had compromised data in an incident that occurred in December. The agency said it was aware of an issue involving servers located outside its core corporate network and had initiated a forensic investigation to better understand the scope and impact of the breach. According to ESA, the affected servers were used to support unclassified collaborative engineering activities within the scientific community.

Multiple reported incidents of GPS spoofing also made headlines, drawing attention to the growing vulnerability of navigation and positioning systems. Reports also highlighted a rise in electronic interference, including GPS jamming and spoofing, in critical maritime chokepoints such as the Persian Gulf and the Strait of Hormuz.

Reports further suggested that for nearly a week in early November, aircraft operating within a 60-nautical-mile radius of New Delhi International Airport experienced counterfeit GNSS signals that indicated incorrect aircraft positions and generated misleading terrain warnings. While alarming, similar incidents have become increasingly common along India's borders with Pakistan and Myanmar, where GNSS spoofing has reportedly been used as a countermeasure against drone operations.

Air France and KLM also confirmed that attackers had breached a customer service platform, resulting in the theft of data belonging to an undisclosed number of customers. The compromised information included names, email addresses, phone numbers, loyalty programme details, and recent transaction records. However, both airlines stated that customers' financial data and other highly sensitive personal information were not affected by the incident. In a separate incident, Hawaiian Airlines also confirmed that a cyberattack had disrupted some of its IT systems.

There were also reports that hackers had leaked the personal data of around five million Qantas customers on the dark web after the airline failed to meet a ransom deadline set by the attackers. The hacker collective Scattered Lapsus$ Hunters posted an extortion notice on a dark web leak site, demanding payment in exchange for withholding the stolen data from public release.

In another incident, RTX Corporation, the parent company of Collins Aerospace, confirmed in a filing with US federal regulators that ransomware was used in a cyberattack targeting its airline passenger processing software. The attack, discovered on September 19, caused flight disruptions across several European hubs, including Heathrow Airport, Brussels Airport, and airports in Berlin and Dublin.

Health Sector No Exception

The World Health Organization(WHO) has observed that the rapid expansion of telemedicine, electronic health records, and other digital health solutions has improved access to care and service delivery in recent years, but it has also significantly increased the healthcare sector's exposure to cybersecurity risks. Healthcare has become one of the most frequently targeted sectors for cyberattacks. Such breaches lead to substantial financial losses, compromise patient privacy, disrupt critical medical services, delay treatments, and in severe cases, pose direct risks to patient safety and lives.

Health insurer Blue Shield of California notified approximately 4.7 million individuals that their protected health information (PHI) was exposed to Google over a period of several years. According to the organisation, the breach resulted from a website misconfiguration that caused members' data to be inadvertently shared with the Google Ads advertising service. The information potentially exposed included names, family size, insurance plan details, city and ZIP code, account identifiers, medical claims information, patient financial responsibility data, and records related to physician searches.

US health and life insurer Aflac disclosed that a cyberattack detected in June affected more than 22.6 million individuals, with personal and claims-related information, including Social Security numbers, potentially accessed. The investigation indicated that the intrusion was likely carried out by the Scattered Spider group.

In another incident, this time in Israel, a serious attempted cyberattack was reported at Shamir Medical Center during Yom Kippur. While the attack did not disrupt hospital operations and all systems remained accessible, authorities raised concerns about the potential leakage of sensitive data. The National Cyber Directorate noted that initial assessments indicated emails sent to and from the hospital on September 25 had been compromised, including messages containing medical information.

Crypto Theft Incidents and Regulatory Steps

More than $3.4 billion was stolen from the cryptocurrency industry in 2025, according to a recent report, with the majority of losses attributed to North Korean hackers. The annual assessment of crypto-related theft highlighted a broader shift towards larger and more costly attacks, alongside the emergence of new techniques used by North Korean actors to launder stolen digital assets. Of the $3.4 billion stolen from the cryptocurrency sector between January and December, the report attributed at least $2.02 billion to hackers linked to North Korea, which is an increase of $681 million compared with the amount they were estimated to have stolen in 2024.

A substantial portion of these losses stemmed from a single incident: the $1.4 billion theft from Dubai-based crypto platform Bybit in February. The cryptocurrency exchange Bybit was hacked for more than $1.4 billion worth of Ethereum in an incident that cybersecurity experts have described as the largest theft ever targeting a crypto platform. The Dubai-based company said the breach occurred during the transfer of funds from a cold wallet, which is where private keys are stored offline for security, to a warm wallet that is connected to the internet, exposing the assets during the transition.

Indian cryptocurrency exchange CoinDCX also suffered a security breach that resulted in the theft of $44.2 million. According to reports, the compromise was limited to an internal operational account and did not affect customer assets. In its first incident report, the company stated that the full financial impact would be absorbed by CoinDCX itself using its treasury reserves, underscoring that customers would not bear any losses from the breach.

It was also reported that the real-world asset (RWA) re-staking protocol Zoth suffered a security exploit that resulted in losses exceeding $8.4 million, prompting the platform to place its website into maintenance mode. According to a security firm's analysis, the protocol's deployer wallet had been compromised, enabling the attacker to withdraw more than $8.4 million worth of crypto assets.

When it came to regulation, the global policy landscape in 2025 looked markedly different from that of 2024. The Markets in Crypto-Assets Regulation (MiCA) came fully into force at the start of 2025, marking a shift from fragmented, nationally driven anti–money laundering regimes to the world's first comprehensive framework for crypto assets. However, despite sustained efforts by EU authorities, including the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA), to develop detailed technical standards and promote supervisory convergence, differences in national interpretation and ongoing implementation challenges continue to persist across member states.

Another major development was the passage of the GENIUS Act in the US, which established a federal regulatory framework for stablecoin issuers. Beyond its domestic impact, the legislation set an international benchmark and helped accelerate global momentum around the development of stablecoin policies.

From a law enforcement perspective, the year marked a positive step forward, with agencies making notable progress in tackling cryptocurrency-related thefts. In November 2025, Europol supported a coordinated action week led by law enforcement authorities from Switzerland and Germany in Zurich. The operation targeted the illicit cryptocurrency mixing service Cryptomixer, which is suspected of enabling cybercrime activities and facilitating money laundering. In India, the Central Bureau of Investigation (CBI) seized cryptocurrencies worth Rs. 23.94 crore after conducting searches at more than 60 locations across five states in connection with the Rs. 6,600 crore GainBitcoin scam. The coordinated searches were carried out at multiple sites across the country as part of the agency's ongoing investigation into the large-scale cryptocurrency fraud.

Cyber Events Against Critical Infrastructure

As mentioned earlier, critical infrastructure sectors such as aviation, healthcare, and space remained under sustained and persistent attack from malicious actors throughout 2025. However, these attacks were not confined to these critical sectors alone, with a wide range of other key sectors also coming under increasing cyber pressure.

Canada's national cybersecurity agency confirmed that hackers had targeted a water facility, tampering with water pressure valves and causing degraded service for the community served by the compromised system. In a separate incident, attackers interfered with an automated tank gauge (ATG) at a Canadian oil and gas company, triggering false alarms. ATG systems, long known to suffer from serious security vulnerabilities, have been targeted by hackers for more than a decade, underscoring the persistent risks facing industrial control systems.

In a separate incident targeting critical national infrastructure, hackers linked to Russia reportedly targeted a hydropower plant in Poland once again, this time disrupting its control systems and turbine operations. Hacktivists released a video that initially appeared to show footage from an earlier intrusion. However, closer analysis indicated that the same group had carried out a fresh attack on the same facility. Based on data collected from the plant's turbines, Polish analysts assessed that the disruption affected live operations, making the incident more damaging than the previous attack, which was believed to have taken place while the plant was offline.

According to reports, hackers have carried out cyberattacks against Britain's drinking water suppliers since the beginning of 2025. While the incidents did not compromise the safety of the water supply itself, they affected the organisations responsible for operating and managing those systems.

Evolving Cybercrimes and Global Response

Cybercrime has evolved into a thriving and highly profitable industry, posing a serious threat to governments, businesses, and individuals worldwide. With nearly two-thirds of the global population now online and large segments of the world economy dependent on information and communications technology, virtually everyone has become a potential target. Advances in technologies such as artificial intelligence and automation have helped fuel an entire underground ecosystem commonly described as cybercrime-as-a-service, lowering the barriers to entry and enabling a wider range of actors to carry out sophisticated attacks.

In one of the more troubling trends, researchers found that cybercriminals are exploiting AI to target organisations more effectively and to develop malicious code, further complicating the threat landscape. AI tools are increasingly enabling cybercriminals with limited technical expertise to generate malicious code. Numerous examples of such code have recently surfaced on underground hacking forums.

According to threat assessments, a range of actors including nation state backed APT groups operating on behalf of the governments of China, Iran, North Korea, and Russia, have attempted to misuse the Gemini AI tool for malicious purposes. Google confirmed that government-linked actors from at least 20 countries had accessed Gemini, with the highest levels of activity traced to groups based in China and Iran.

As noted in earlier sections, there was also a marked surge in ransomware-related incidents, along with a rise in data breaches linked to organised criminal groups. Retailers also found themselves increasingly on the receiving end of cyberattacks, as illustrated by the case involving Marks & Spencer. A broader pattern emerged in which retailers were frequently placed in the crosshairs of threat actors. It was also noted that attackers often exploit the seasonal nature of the retail sector to maximise pressure on victims.

The global response was equally significant, with law enforcement agencies carrying out seizures, arrests, and coordinated operations to dismantle the infrastructure used to carry out cybercrime. The response also extended to governance and regulation, with governments and regulatory bodies strengthening policy frameworks to address emerging cyber and digital risks.

The most consequential collective governance step came when 72 countries signed a landmark United Nations cybercrime treaty in Hanoi. The agreement seeks to strengthen global efforts to combat cybercrime by criminalising a broad range of cyber-dependent and cyber-enabled offences, improving cross-border sharing of electronic evidence, and establishing a 24/7 cooperation network among participating states. Significantly, the treaty also set a historic precedent by becoming the first international agreement to recognise the non-consensual dissemination of intimate images as a criminal offence, marking an important step forward for the protection of victims of online abuse.

In a major INTERPOL-coordinated operation, law enforcement authorities across Africa arrested 1,209 cybercriminals linked to attacks on nearly 88,000 victims. The crackdown led to the recovery of USD 97.4 million and the dismantling of 11,432 malicious infrastructure, highlighting both the global scale of cybercrime and the pressing need for sustained cross-border cooperation.

Known as Operation Serengeti 2.0, the initiative ran from June to August 2025 and brought together investigators from 18 African countries alongside the United Kingdom. The operation focused on high-impact cyber threats, including ransomware, online fraud, and business email compromise (BEC), marking one of the most extensive coordinated cybercrime enforcement efforts in the region.

In another INTERPOL-coordinated operation, law enforcement agencies across 19 countries arrested 574 suspects and recovered approximately USD 3 million in a major cybercrime crackdown across Africa. The operation focused on three of the most prevalent forms of cybercrime, including BEC, digital extortion, and ransomware. As part of the coordinated effort, authorities also dismantled more than 6,000 malicious links and successfully decrypted six separate ransomware variants, significantly disrupting ongoing criminal activity.

In November 2025, the latest phase of Europol's Operation Endgame was coordinated from its headquarters in The Hague. The operation targeted several major cybercrime enablers, including the infostealer Rhadamanthys, the VenomRAT remote access trojan, and the Elysium botnet, all of which played a significant role in international cybercriminal activity. Authorities successfully dismantled these three platforms, dealing a major blow to the cybercrime ecosystem. In addition, the primary suspect linked to VenomRAT was arrested in Greece on 3 November 2025, marking a key enforcement success.

Cyber Crime Compounds and Law Enforcement Actions

The year 2025 also saw a rise in criminal activity linked to cyber scam compounds, particularly across parts of Asia. Particularly, cyber scam operations have surged across Southeast Asia since the onset of the COVID-19 pandemic, evolving into a transnational organised crime crisis of overwhelming scale and complexity.

At the core of many of these scam compounds are so-called pig-butchering schemes, in which scammers patiently build online relationships with victims before persuading them to part with their money, often under the guise of cryptocurrency or other investment opportunities. As discussed earlier, these operations have become increasingly sophisticated, with criminals leveraging generative AI to translate and sustain conversations, deepfake technology to conduct convincing video calls, and mirrored websites designed to closely imitate legitimate investment platforms. According to an assessment by the US Government, scams originating from Southeast Asia surged sharply, costing Americans more than $10 billion in losses in 2024 alone.

In response, authorities across South East Asia, along with major powers such as the US, launched decisive crackdowns against these organised criminal groups, intensifying law enforcement action and cross-border cooperation to disrupt their operations. In September 2025, the Office of Foreign Assets Control (OFAC) of the United States Department of the Treasury imposed sanctions on a large network of scam centres operating across Southeast

Asia, accused of stealing billions of dollars from its citizens through forced labour and violence. The sanctions targeted nine entities operating in Shwe Kokko, Myanmar, a well-known hub for cryptocurrency investment scams reportedly operating under the protection of the OFAC-designated Karen National Army. An additional ten targets based in Cambodia were also sanctioned as part of the action.

In another law enforcement operation, Thailand decided to cut the electricity supply to certain border areas with Myanmar to combat scam centers, responding to increasing pressure on these illegal compounds that have trapped numerous individuals of various nationalities. The United Nations reports that criminal gangs have trafficked hundreds of thousands across Southeast Asia, forcing them into fraudulent online operations, including those near the Thai-Myanmar border.

The Philippine National Bureau of Investigation (NBI) raided an alleged "love scam" operation in a Makati condominium, apprehending up to 100 Filipinos and a Chinese national. NBI Director Jaime Santiago revealed that the suspects leveraged artificial intelligence (AI) to carry out online romance scams. Leading the raid, Santiago stated that agents uncovered the use of AI-generated conversations and fake profile pictures of attractive women to deceive victims into fraudulent cryptocurrency schemes.

The U.S. and U.K. launched a coordinated operation against Cambodian tycoon Chen Zhi, chairman of Prince Group, over alleged forced-labour scam networks. The U.S. Department of Justice filed its largest-ever forfeiture action, seizing about 127,271 Bitcoin worth roughly $15 billion. Separately, SpaceX disabled more than 2,500 Starlink terminals linked to scam centers in Myanmar, including sites such as KK Park. These steps aim to disrupt criminal networks built on illicit finance and human trafficking.

Law enforcement operations in India have also been effective in identifying perpetrators and bringing them to justice. In one such operation, police arrested 42 individuals in Delhi as part of a special drive against cybercrime for their alleged role in multiple inter-state fraud modules that collectively defrauded victims of more than Rs. 254 crore. The arrests were carried out during raids conducted under Operation CyHawk. During the operation, authorities recovered three laptops, two computer systems, 43 mobile phones, 17 passbooks, two cheque books, 14 debit cards, and ₹1.6 lakh in cash. Police also confirmed that the crackdown focused on networks involved in ATM fraud, so-called digital arrest scams, job-related fraud, digital marketing scams, USDT-based money laundering, cheque-withdrawal rackets, and extensive mule-account networks operating across Indian states of Delhi, Uttar Pradesh, and Haryana.

In another notable enforcement success, a coordinated operation led by India's CBI, acting on intelligence shared by the FBI, dismantled a major cybercrime syndicate operating from Noida. Six individuals were arrested for their alleged role in defrauding US citizens of nearly USD 8.5 million over a three-year period.

The CBI carried out a series of raids in December across multiple locations in Noida, Delhi, and Kolkata. The searches led to the seizure of Rs. 1.88 crore in cash, 34 electronic devices including mobile phones and laptops and several documents connected to the fraudulent activities. The crackdown formed part of a broader initiative codenamed Operation Chakra.

The Supreme Court has also asked the CBI to lead a nationwide investigation into these increasingly sophisticated frauds, noting that digital-arrest scams often involve callers impersonating police, courts, or government agencies to intimidate victims over audio or video calls and extort money. It further directed information-technology intermediaries to fully cooperate with the CBI and furnish all relevant data for ongoing and future investigations into such scams. The government has also set up a high-level inter-departmental committee, headed by the special secretary (Internal Security), Union Ministry of Home Affairs, to comprehensively examine all aspects of digital arrests in the country. The first meeting of the committee in December was attended by officials from the Indian Cyber Crime Coordination Centre, the Reserve Bank of India, the Department of Telecommunications, and the Ministry of Electronics and Information Technology.

Cyber Espionage Operations

Government and military institutions continue to face sustained intrusion attempts aimed at intelligence collection and operational disruption. Technology and manufacturing sectors, particularly aerospace and semiconductors, remain prime targets of espionage-driven campaigns. Financial services, including banks and cryptocurrency exchanges, are under constant pressure from financially motivated actors. Healthcare and academic institutions, likewise, are now routinely targeted due to the high value of personal data and sensitive research assets.

China and North Korea remain dominant actors in cyber-espionage campaigns. North Korea's targeting of defence companies for industrial espionage has emerged as a key driver in its efforts to acquire critical military technologies. In this strategy, the infiltration of IT workers has become an increasingly important and evolving tool, supporting both financial gain and intelligence collection objectives. In February 2025, hackers linked to North Korea carried out an espionage campaign targeting South Korean entities, exfiltrating system reconnaissance data from potentially thousands of compromised machines.

By April 2025, North Korean cyber operatives were reported to have expanded these infiltration efforts beyond the Korean Peninsula, increasingly targeting defence and government organisations across Europe, signalling a broader geographic scope for their espionage operations. In May 2025, a hacker group known as APT37 was reported to have launched a new espionage campaign targeting organisations in South Korea with links to national security.

APT37 is widely assessed to be state-sponsored by North Korea and has a history of targeting high-profile individuals as well as public and private sector entities, primarily within South Korea. Allegedly operating under the Ministry of State Security, the group is considered one of Pyongyang's most active cyber units and is particularly known for its reliance on social engineering techniques to trick victims into opening malicious files.

In another reported operation, this time in the United States, North Korean cyber operatives allegedly established two front companies in violation of Treasury sanctions to compromise developers working in the cryptocurrency sector with malicious software. The firms were reportedly registered in New Mexico and New York, using fabricated identities and addresses to mask their true origins. According to reports, the hackers were linked to a subgroup of the Lazarus Group, an elite North Korean cyber unit operating under the Reconnaissance General Bureau, Pyongyang's primary foreign intelligence service.

According to government reports, state-sponsored cyber threat actors from China were actively targeting networks worldwide, spanning sectors such as telecommunications, government, transportation, hospitality, and military infrastructure. These actors have primarily focused on core backbone routers operated by major telecommunications providers. In addition, they have increasingly exploited compromised devices and trusted network connections to pivot laterally into adjacent systems, enabling broader and more persistent access across targeted networks.

Over time, China's cyber operations have shifted from a primary focus on economic espionage to more strategic and politically driven campaigns, posing increasingly serious challenges to global security. China's espionage operations drew renewed attention in 2025, continuing a pattern seen in previous years. Assessments of cyber and critical infrastructure security highlighted sector-specific risks, noting that intrusions across US energy, water, telecommunications, transportation, and healthcare systems point to sustained espionage by China–linked 'Typhoon' threat actors. According to these reports, such state-sponsored cyber activities suggest preparations for potential future conflicts, with a focus on gaining access to critical systems in advance. The intent appears to be the ability to disrupt logistics, delay military deployments, and interfere with essential civilian infrastructure, underscoring the strategic and long-term nature of Beijing's cyber operations.

A leading AI company also reported that it had disrupted a China-backed cyber-espionage campaign that infiltrated financial institutions and government agencies with minimal human involvement. According to the company, its AI-powered coding tool was manipulated by a Chinese state-sponsored group in September to target around 30 organisations worldwide, with the campaign achieving a limited number of successful intrusions before it was detected and halted. The Australian spy chief warned that hackers linked to China's government and military were actively targeting Australia's critical infrastructure. The warning noted that the country was facing a growing risk of "high-impact sabotage." According to the assessment, what were described as unprecedented levels of espionage have significantly increased the likelihood of cyber-enabled sabotage, with the threat expected to intensify over the next five years.

Iranian cyber operators were similarly sophisticated, if not more so, in their cyber-espionage activities. An Iranian state-sponsored hacking group linked to the IRGC was connected to a spear-phishing campaign targeting journalists, prominent cybersecurity experts, and computer science professors in Israel. According to a report, attackers in several campaigns impersonated fictitious assistants to technology executives or researchers, contacting Israeli technology and cybersecurity professionals via email and WhatsApp. Victims who engaged were redirected to fraudulent Gmail login pages or fake Google Meet invitations designed to harvest credentials.

Many of these campaigns have been attributed to APT35, also known as Charming Kitten. This group is also well known for conducting sustained espionage operations against Iranian dissidents, journalists, and activists, particularly those living outside Iran, using targeted social engineering and credential-harvesting techniques.

In another cyber-espionage–related incident, Russia’s aerospace and defence industries were targeted in a campaign that deployed a backdoor malware known as EAGLET to enable covert data exfiltration. According to reports, technology companies in Russia involved in air defence systems, sensitive electronics, and other defence-related applications were also targeted by a cyber-espionage group. The attackers reportedly used AI-generated decoy documents to deceive victims and facilitate espionage operations.

State of Emerging Technologies

Every year, remarkable innovations continue to emerge from research laboratories around the world, steadily pushing the boundaries of technology and possibility. Global adoption of AI continued to accelerate in 2025, with roughly one in six people worldwide now using generative AI tools, which is a striking level of uptake for a technology that only recently entered mainstream use. Countries that made early investments in digital infrastructure, AI skills development, and government adoption, such as the United Arab Emirates (UAE), Singapore, Norway, Ireland, France, and Spain, continued to lead in AI adoption. Among them, the UAE further extended its global lead, according to an assessment on AI adoption.

Investment in quantum technologies is accelerating rapidly, with breakthroughs emerging at an increasing pace. Reflecting the growing global significance of the field, the United Nations designated 2025 as the International Year of Quantum Science and Technology, marking a century since the foundational development of quantum mechanics. Google announced that it has developed a new computer algorithm that could pave the way for practical applications of quantum computing, including the ability to generate unique data for use in AI systems. The algorithm, known as Quantum Echoes, runs on the company’s quantum chip and was reported to be around 13,000 times faster than the most advanced classical algorithms on supercomputers, highlighting a significant leap in quantum computing performance.

Microsoft also unveiled a new quantum chip, signalling that a fundamental shift in computing technology may be closer than previously thought. The company stated that its Majorana 1 chip is significantly less prone to errors than competing approaches, which is one of the central challenges in quantum computing.

International Developments In Cyber Cooperation

International Cooperation

For the first time, UN Security Council members met to discuss the threat of commercial spyware. At the informal Arria-formula meeting, a senior US diplomat urged stronger efforts to secure justice for victims, while other nations pledged action. The discussion comes amid growing concerns over spyware infecting diplomats' devices. China and Russia opposed the US-led hearing, with China emphasizing the need to focus on nation-state cyberweapons like the Stuxnet virus used against Iran's nuclear program. Russia called for a broader UN discussion on spyware.

Representatives from 20 allied governments and national agencies took part in a NATO-led exercise held from April 7 to 11, aimed at strengthening mutual cyber support among allies. The exercise focused on improving coordination and enhancing collective responses to major malicious cyber activities targeting critical national infrastructure. Through simulated complex cyber threat scenarios, participants practiced real-time information sharing, joint decision-making, and coordinated response measures, reinforcing NATO's commitment to collective cyber defence and resilience across the alliance.

At a meeting held in Brasília, the BRICS countries discussed coordinated measures to strengthen cybersecurity and enhance the sharing of information and best practices. The discussions reflected a shared objective to reduce reliance on foreign technological solutions and advance a more inclusive approach to digital governance, with particular emphasis on rapid and coordinated responses to transnational cyber threats.

Singapore hosted the 5th International Counter Ransomware Initiative (CRI) Summit on 24 October 2025, held alongside Singapore International Cyber Week 2025. The summit brought together nearly 150 participants from 60 countries, as well as representatives from international organisations and the private sector, underscoring the depth of global cooperation in addressing the ransomware threat. At the conclusion of the Summit, the CRI Steering Committee issued a summary reaffirming its collective commitment to strengthen resilience against ransomware threats. The statement underscored pledges to support members facing ransomware incidents, hold criminal actors accountable and deny them safe havens, and promote responsible state behaviour in cyberspace.

Developments in cyber and tech governance worldwide

The UK government took the initiative to criminalize the creation and distribution of sexually explicit deepfake images. This move aims to combat the rising spread of such content, which primarily targets women and girls. While Britain outlawed the sharing of intimate photos or videos without consent, commonly known as revenge porn, in 2015, the existing legislation does not address fake images. The UK government also considered a ban on all public bodies from making ransomware payments as part of efforts to combat cyber threats. Under the plan, critical national infrastructure operators will be prohibited from complying with ransom demands when hackers seize IT systems. Private companies will be required to report such payments to the government, with transactions potentially blocked if they involve sanctioned entities or foreign states. If enacted, the proposals will also make reporting ransomware attacks mandatory.

Australia introduced a restriction banning children under the age of 16 from using major social media platforms, including TikTok, X, Facebook, Instagram, YouTube, Snapchat, and Threads.Under the new rules, minors are prohibited from creating new accounts, while existing profiles belonging to under-16 users have been deactivated. The move is being described as the first ban of its kind globally, marking a significant shift in how governments regulate children's access to social media. The decision was supported by findings from a government-commissioned study conducted in 2025, which showed that 96% of children aged 10 to 15 were active on social media. The study also found that seven in ten of these children had been exposed to harmful content, including misogynistic and violent material, as well as posts promoting eating disorders and suicide.

A cybersecurity bill introduced in the Turkish Parliament also faced strong criticism, with concerns raised about potential threats to human rights and personal freedoms. While the bill seeks to strengthen the country's defenses against rising cyber threats, it has raised alarms over surveillance, data privacy, and the consolidation of power within government institutions. The proposed legislation grants broad powers to the newly established directorate, including the authority to collect and store extensive data from public institutions and critical infrastructure providers

Japan's Parliament has passed a bill enabling the government to take proactive measures to prevent major cyberattacks. The Upper House approved the active cyber defense legislation with support from both the ruling coalition and the opposition Constitutional Democratic Party. A key provision, respecting the secrecy of communications, was added during Lower House deliberations. The law, set to take full effect in 2027, aligns with Japan's 2022 National Security Strategy, which aims to match or exceed the cyberdefense capabilities of major Western nations. Under the new framework, the government will monitor and analyze international communications involving Japan, even during peacetime. If signs of a cyberattack emerge, police and the Self-Defense Forces will be authorized to take countermeasures. Joint police–SDF bases will be established, and public-private cooperation will be promoted through sensitive information sharing. Infrastructure operators will also be required to report cyberattacks.

In response to the recent military and cyber escalation between Israel and Iran, Germany plans to deepen its cybersecurity cooperation with Israel and establish a joint cyber research center. According to reports, German Interior Minister Alexander Dobrindt unveiled the initiative during a visit to Israel. Dubbed the Cyber Dome, the plan includes the creation of a German-Israeli cyber research center, enhanced collaboration between Israel's Mossad and Germany's BND intelligence agency, strengthened cyber and anti-drone defenses, and the development of a nationwide emergency alert and civil shelter system modeled after Israel's.

Major Cyber Developments in the South Asian Region

India

- Amid rising digital threats, the Indian Home Ministry has urged every Indian city to appoint a Chief Information Security Officer (CISO) to safeguard critical systems and citizen data. With the rapid expansion of smart cities, the initiative aims to build in-house cyber resilience beyond reliance on private consultants and thirdparty vendors. During a high-level meeting on cybersecurity preparedness in New Delhi, Union Home Secretary Govind Mohan emphasized the urgent need for dedicated CISOs in each city to defend local digital infrastructure and data from evolving cyber threats.

- India's Chief of Defence Staff General Anil Chauhan and the Secretary of the Department of Military Affairs unveiled the declassified Joint Doctrine for Cyberspace Operations during the Chiefs of Staff Committee meeting in New Delhi. The move highlights India's resolve to strengthen transparency, accessibility, and the wider dissemination of joint warfighting concepts. The doctrine sets a unified framework for safeguarding national cyberspace interests by integrating offensive and defensive capabilities, ensuring synchronised operations across the three Services.

- In January, there were reports that Tata Technologies Ltd. suspended some of its IT services following a ransomware attack that affected the company's network. The company confirmed that the attack temporarily impacted IT assets, which were restored. Despite the cyberattack, client delivery services remained fully operational, with no disruption to customer operations.

- Hindustan Aeronautics Limited (HAL) fell victim to a cyber fraud scheme in which scammers, posing as a U.S.- based company, deceived the organization into transferring Rs. 55 lakh. The fraud was uncovered when HAL realized the payment had been sent to the wrong account. The scam came to light after PS Engineering, the intended recipient, reported that they had not received the payment. Upon investigation, HAL discovered that the email ID used in the transaction was fraudulent.

- Indian stockbroker Angel One confirmed that some of its Amazon Web Services (AWS) resources were compromised and that it engaged an external forensic firm to assess the impact of the incident. Following the disclosure, Angel One's shares extended their decline, falling by as much as 4.7%. The company said it was alerted to the breach by its dark-web monitoring partner and responded by immediately resetting all credentials across its AWS cloud environment and other applications.

- In a cyber incident reported to have taken place in June, the servers of two hospitals in New Delhi were compromised. What was initially believed to be a technical malfunction was later confirmed by IT teams to be a deliberate cyberattack. At one of the affected hospitals, the breach caused major operational disruptions, impacting electronic medical records, billing systems, and appointment scheduling platforms. At the other facility, investigators confirmed unauthorised access to patient data, financial records, and administrative files, heightening concerns over a possible data breach and exposure of sensitive information.

- The Indian Council of Agricultural Research (ICAR), India's apex agricultural research body, reportedly suffered a cybersecurity breach that resulted in the loss of critical data spanning areas such as recruitment processes and research projects. According to reports, ICAR subsequently set up a six-member committee to examine issues linked to the non-functionality of its Data Centre (DC) and Disaster Recovery Centre (DRC). The committee was tasked with submitting recommendations, proposing appropriate measures to strengthen data security, and identifying steps to prevent similar incidents in the future.

- The website of Nippon Life India Mutual Fund was targeted in a cyberattack. The following day, the company informed stock exchanges about the incident, confirming that its IT infrastructure had been compromised. While no timeline was provided for the website's restoration, the management assured that efforts were underway to resolve the issue promptly.

- A major cyberattack took down the official website of Uttar Haryana Bijli Vitran Nigam Limited (UHBVNL), disrupting key online services, including new electricity connections, and impacting over 50,000 consumers. Senior officials confirmed the breach, stating that a wide range of consumer services had been affected. Cybersecurity teams were working around the clock to contain the damage and restore normal operations.

- Indian grocery delivery startup KiranaPro suffered a major cyberattack, resulting in the complete wipeout of its data, the company's founder confirmed to media. The breach destroyed critical assets, including app code and servers holding sensitive customer information such as names, addresses, and payment details. While the app remains online, it is currently unable to process orders.

- Indian cryptocurrency exchange CoinDCX suffered a $44 million loss in a suspected sophisticated server breach. One of its employees has been arrested in connection with the hack. The stolen cryptocurrency was routed through multiple wallets to evade detection, complicating efforts to trace it. Police later uncovered evidence suggesting insider involvement and arrested a CoinDCX employee during the investigation.

- The Indian government has confirmed that seven major airports were impacted by cyberattacks, including Delhi, where incoming flights reported GPS spoofing. Airports in Mumbai, Kolkata, Hyderabad, and Bengaluru were also affected. Officials said no flights were disrupted despite the spoofing attempts. In response, all Indian airlines have completed the necessary software upgrades, allowing their aircraft to safely resume commercial operations.

PAKISTAN

- Pakistan passed the Cybersecurity Act 2025 in November 2025. The Act created a new National Cybersecurity Authority (NCA) to lead nationwide incident response and threat-intelligence operations, while expanding the role of the Pakistan Computer Emergency Response Team (PKCERT) and supporting secure digital-public-infrastructure initiatives under the Digital Economy Enhancement Project.

- Pakistan's opposition in January 2025 expressed concerns over the government's proposed social media controls, fearing it would further suppress freedom of speech. The proposal includes blocking platforms and imprisoning users for spreading disinformation. The Prevention of Electronic Crimes Act, introduced by Pakistan's Law Minister, would establish an agency with the authority to block unlawful and offensive content on social media and ban individuals or organizations. Social media platforms would be required to register with the new Social Media Protection and Regulatory Authority, facing potential temporary or permanent bans for non-compliance.

- According to reports, digital devices in Pakistan have increasingly become prime targets for cybercriminal activity. A cybersecurity assessment revealed that more than 5.3 million on-device attacks were detected in the country during the first three quarters of 2025 alone (January to September), highlighting the scale and seriousness of the threat. The report further noted that APT groups have increasingly focused on Pakistan, with as many as seven such groups targeting sectors including telecommunications and financial services, critical infrastructure, defence, and government institutions, in addition to private organisations.

- Ministry of Interior ordered an investigation into a sensitive data breach affecting thousands of Pakistani nationals, the government confirmed. The move followed reports by a local broadcaster that personal data belonging to a wide range of individuals including federal ministers and senior officials had been compromised and was being offered for sale online. According to the reports, the leaked information included mobile phone subscriber addresses, call records, copies of national identity cards, and details of foreign travel.

BANGLADESH

- Bangladesh's interim government approved the Cyber Security Ordinance 2025 in May 2025, a major overhaul of the earlier Cyber Security Act 2023, repealing nine controversial sections and making around 95% of existing cases under the old law automatically void. The new ordinance significantly softened penalties, made all speech-related offences bailable, reduced maximum imprisonment to two years, and increased punishment for filing false cases. It also recognises internet access as a civic right, criminalises online gambling, and introduces new offences such as online sexual harassment, incitement of religious hatred, and cybercrimes committed using artificial intelligence—a first in South Asia. Magistrates are empowered to dismiss baseless cases within 24 hours, and a new content-removal authority with civil-society representation must seek court approval within 72 hours for takedowns, ensuring greater transparency and safeguards against misuse.

- According to an assessment, Bangladesh’s banking sector faced mounting cyber threats, with an average of more than 400 cyberattacks occurring each day. Research indicated that a significant share of these attacks originated from overseas, particularly from China, North Korea, and Russia, with China alone responsible for roughly one-quarter of the total attacks.The findings highlighted the increasing vulnerability of Bangladesh’s digital banking infrastructure and underscored the urgent need to strengthen cybersecurity capabilities and protective measures across the sector.

Afghanistan

- The Taliban Ministry of Communications confirmed that documents from several government departments were exposed in what it described as an unprecedented cyber breach. According to the ministry, preliminary investigations indicate that the documents were obtained sporadically from individual computers that lacked adequate security protections, rather than through a single coordinated intrusion. Taliban officials nonetheless maintained that the central government database itself had not been compromised.

Nepal

- Social media played a central role in the unrest in Nepal, where authorities lifted a ban on online platforms after it triggered widespread anti-corruption protests that escalated into clashes with police. When the government moved to block 26 social media platforms, including Facebook and YouTube, protests erupted. Thousands of young demonstrators reportedly stormed parliament in Kathmandu, prompting curfews in several districts. Days before protests erupted in Nepal, the government announced a ban on most social media platforms, citing their failure to meet a registration deadline. Officials said the move was aimed at curbing fake news and hate speech. However, many young Nepalese perceived the decision as an effort to stifle dissent and silence their voices.

Sri Lanka

- Sri Lanka’s Cabinet approved a new National Cyber Protection Strategy (2025–2029), marking a major upgrade of its earlier 2018–2023 framework and signalling a renewed push to strengthen national cyber-resilience. The plan—developed by Sri Lanka CERT with World Bank support—focuses on modernising outdated cyber laws, improving incident-response capacity, enhancing coordination across state institutions, and expanding public-private cooperation. It also emphasises workforce development, education, and awareness, while deliberately keeping the strategy civilian-focused to build public trust. Building on the foundations of the previous strategy, the new plan responds to rising threats linked to digital finance, cloud adoption, AI, and geopolitical cyber risks, positioning cybersecurity as a central pillar of Sri Lanka's broader digital-transformation agenda.

INDIA'S CYBER GOVERNANCE

- The Ministry of Electronics and Information Technology (MeitY) took a significant step towards technological self-reliance by launching an indigenous web browser under the Atmanirbhar Bharat initiative. Aimed at encouraging domestic innovation and strengthening India's digital sovereignty, the project was developed by the Centre for Development of Advanced Computing (C-DAC), Bengaluru, underscoring a strategic push to reduce dependence on foreign digital technologies.

- Telangana's IT Minister, D. Sridhar Babu, announced that the state government will introduce a cybersecurity policy aligned with India's Digital Personal Data Protection Act. Speaking at the Cyber Security Conclave 2025, he highlighted Telangana's proactive approach to building a robust cybersecurity ecosystem and countering cyber threats. The government is also in talks to establish a Cyber Defence Centre in Hyderabad to protect both citizens and government entities from cyber risks.

- The first batch of cyber commandos, formed under the Indian Cyber Crime Coordination Centre (I4C), completed a six-month training program at the Indian Institute of Information Technology (IIIT) in Kottayam. Comprising 30 commandos selected from various state police forces across India, the trainees were chosen through a nationwide entrance exam. They received advanced training in cyber defense strategies, ethical hacking, digital forensics, and penetration testing to strengthen the country's digital security framework.

- Karnataka has become the first state in India to establish a dedicated Cyber Command Centre, setting a national precedent in tackling a wide range of digital threats. This comprehensive centre will address various aspects of cybersecurity and cybercrime, including ransomware, online crimes against women and children, sextortion, digital frauds, deepfakes, identity theft, hacking, data breaches, digital arrests, stalking, and disinformation. It aims to serve as a centralized hub for prevention, response, and outreach in the fight against evolving cyber threats.

- Standardisation Testing and Quality Certification (STQC) is now mandatory for CCTV cameras in India to ensure compliance with cybersecurity, quality, and safety standards. The certification aims to prevent data leaks, including attempts to extract footage through software modifications. Licenses will be granted only after authorities verify that there are no loopholes allowing surveillance data from India to be transmitted to foreign servers

- In a major move to curb the misuse of telecom resources in cybercrimes and financial fraud, the Department of Telecommunications (DoT) and the Financial Intelligence Unit–India (FIUIND) have signed a comprehensive Memorandum of Understanding (MoU) to strengthen information sharing and coordination.The enhanced datasharing framework will leverage advanced technology platforms, including the DoT's Digital Intelligence Platform (DIP) and FIU-IND's Finnex 2.0 portal. These system-based exchange portals will enable secure, real-time transmission of information between the two agencies.

- Amid rising cyber thefts, the Indian government made cybersecurity audits mandatory for all cryptocurrency exchanges and custodians. Platforms must engage a security auditor registered with the Indian Computer Emergency Response Team (CERT-In), the national agency handling cybersecurity incidents. Additionally, registration with India's anti-money laundering authority, the Financial Intelligence Unit (FIU), now requires all virtual digital asset (VDA) service providers to comply with this rule. According to reports, FIU-designated directors, principal officers, and chief compliance officers of these firms are expected to implement the measures immediately.

- The MeitY has unveiled India's AI Governance Guidelines under the IndiaAI Mission to promote safe, inclusive, and responsible adoption of AI across sectors. The release marks a major milestone ahead of the India-AI Impact Summit 2026, reinforcing India's leadership in responsible AI governance. The guidelines outline a strong governance framework aimed at fostering innovation while ensuring that AI is developed and deployed safely and ethically.

- The Government of India has notified the Digital Personal Data Protection (DPDP) Rules, 2025, completing the implementation of the DPDP Act, 2023. Together, the Act and the new Rules provide a simple, citizen-centric, and innovation-friendly framework for the responsible handling of digital personal data. Passed by Parliament on 11 August 2023, the DPDP Act sets out a comprehensive system for safeguarding digital personal data, defining the responsibilities of Data Fiduciaries and the rights and duties of Data Principals.

- India's Department of Telecommunications (DoT) issued a regulation requiring WhatsApp and other OTT communication apps like Telegram and Signal to remain continuously linked to users' SIM cards, with platforms given 90 days to comply. The directive also mandates automatic six-hour logouts on web and desktop versions, requiring re-authentication via QR code pairing. The move aims to curb fraud and anonymous misuse by ensuring accountability, as current systems allow apps to function even if a SIM is removed or deactivated. Telecom operators, represented by COAI, support the measure, arguing it will reduce spam and financial fraud while strengthening digital security.

- The Government of India withdrew a directive requiring smartphone makers to preload the Sanchar Saathi cybersecurity app on new devices, following backlash from opposition parties, privacy advocates, and global tech firms over surveillance concerns. The rollback came a day after ministers defended the plan as a tool to track stolen phones and protect users from cyber threats.

INDIA'S CYBER DIPLOMACY

- India and the United States signed a new MoU on Cybercrime Investigations on 17 January 2025 to deepen operational cooperation between their law enforcement and homeland security agencies. Signed by India's Ambassador Vinay Kwatra and the U.S. Acting Deputy Secretary of Homeland Security Kristie Canegallo, the agreement designates India's Indian Cybercrime Coordination Centre (I4C) and the U.S. Department of Homeland Security, including ICE and the HSI Cyber Crimes Center, as the implementing bodies. The MoU enables both sides to expand collaboration in cyber-threat intelligence, digital forensics, and training, recognising that cybercrime increasingly intersects with terrorism, extremism, drug trafficking, human trafficking, money laundering, and other transnational security challenges.

- India and Australia are in early-stage discussions to establish real-time information sharing to combat cybercrime, amid rising threats from state-backed actors like North Korea targeting critical infrastructure such as power grids and healthcare systems. Brendan Dowling, Australia's Ambassador for Cyber Affairs and Critical Technologies, confirmed in an interview that both nations are showing strong interest in a bilateral treaty focused on data-sharing to strengthen their cybercrime response capabilities.

- India's CERT in collaboration with the Ministry of External Affairs, hosted a cybersecurity familiarisation and interactive session for visiting journalists from Europe, the Americas, and Central Asia. The session highlighted CERT-In's continuous cyber drills, capacity-building efforts, and international cooperation including joint exercises and work with France's ANSSI on a high-level AI cyber risk report titled "Building Trust in AI Through a Cyber Risk-Based Approach."

- The Eighth India–EU Cyber Dialogue was held on 20 March 2025 in New Delhi. During the dialogue, both sides reviewed the evolving cyber threat landscape and exchanged views on recent developments in cyber policies, security standards, and the protection of critical information infrastructure. Discussions also covered cooperation in multilateral forums on ICT security, collaboration on 6G standardisation, telecom equipment security standards, and joint capacity-building initiatives.

- India and the United Kingdom held the 1st Strategic Exports and Technology Cooperation Dialogue in New Delhi on 3 June 2025, led by Foreign Secretary Vikram Misri and UK Permanent Under-Secretary Sir Oliver Robbins. The Dialogue focused on "addressing export controls for enabling greater technology cooperation in strategic sectors". This dialogue is aimed at building mutual understanding of systems and agreeing on areas for future cooperation in key sectors such as technology and defence.

2025 stands as a testament to the fact that digital vulnerabilities are persistent, systemic forces that continuously shape the global security environment. The year was defined by a profound shift in the threat architecture, where artificial intelligence transitioned from an emerging technology to a primary weapon for sophisticated phishing, deepfakes, and automated intrusions, affecting roughly 87% of organizations. Ransomware continued to be a direct threat to national resilience, with a 34% increase in attacks on critical sectors such as healthcare, energy, and transportation.

The convergence of physical and digital warfare became an undeniable reality as cyber operations played integral roles in conflicts involving Russia, Ukraine, Israel, and Iran. Simultaneously, financial sectors—particularly cryptocurrency—faced unprecedented pressure, with losses exceeding $3.4 billion, much of which was driven by state-linked actors like North Korea. However, 2025 also marked a turning point in global cooperation. The signing of the landmark UN cybercrime treaty in Hanoi and the success of coordinated international law enforcement actions like Operation Serengeti 2.0 demonstrated a growing collective resolve to dismantle criminal infrastructures. However, this still remain few and far between. Looking forward, there are multiple challenges emerging, from that of ensuring we stay on the right side of agentic AI to mainstreaming quantum safe cryptography. Ultimately, maintaining security in an interconnected world requires not just advanced technical defenses, but also robust, cross-border governance of emerging cyber-technologies.

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

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

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