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

CYBER *Digest*

February 2026

- **UK Government Unveils Cyber Action Plan**
- **France Releases Five-Year National Cybersecurity Strategy**
- **Sedgwick Acknowledges Breach at Contractor Subsidiary**
- **Israel Advances New Cyber Law**
- **UK–China Hold Talks on Joint Cybersecurity Forum**
- **Pakistan-linked Cyberespionage against India**
- **Hacker Steals $282M in Crypto through Social-Engineering Attack**
- **India File**

UK Government Unveils Cyber Action Plan

The Government Cyber Action Plan released on January 6 outlines the UK government's approach to safeguarding public services, ensuring they remain secure, reliable, and resilient.[1] It forms a core component of the wider Roadmap for a Modern Digital Government. The plan has been developed by the Department for Science, Innovation and Technology (DSIT) in close collaboration with government departments, public sector bodies, industry stakeholders, and the Government Cyber Advisory Board (GCAB). It establishes clear, outcome-driven expectations for how government organisations across the public sector should strengthen cyber security and resilience, supported by defined and measurable objectives. The action plan also explains how the UK government will change the way it operates to address the growing cybersecurity and resilience challenges it faces, supported by a strong and proactive central function within the Government Cyber Unit.

France Releases Five-Year National Cybersecurity Strategy

France's new five-year national cybersecurity strategy, released on 29 January 2026, represents a major reset of its national posture, combining sovereignty, EU-level coordination, and large-scale capability building. It builds on ANSSI's 2025–2027 strategic plan and the broader 2026–2030 national cybersecurity strategy, both of which respond to rising geopolitical tensions, AI-driven threats, and lessons learned from major French cyber incidents.

The national cybersecurity strategy is built around five core pillars, each with distinct objectives.[2] While Pillar 1 focuses on positioning France as Europe's largest hub for cyber talent, Pillars 2 and 3 emphasise strengthening national cyber resilience and curbing the growth of cyber threats, respectively. Pillar 4 of the strategy reflects France's ambition to control its technological dependencies while preserving its autonomy of judgement and freedom of action in cyberspace. To achieve this, it aims to maintain and further develop its command of critical cybersecurity technologies and independent assessment capabilities, while also supporting the consolidation of world-leading cyber industrial players at the European level. Pillar 5 focuses on promoting stability and security in cyberspace, both across Europe and at the international level.

Sedgwick Acknowledges Breach at Contractor Subsidiary

Claims administration and risk management firm Sedgwick has confirmed that its federal contracting subsidiary, Sedgwick Government Solutions, suffered a cybersecurity breach.[3] Agencies using Sedgwick Government Solutions include the Cybersecurity and Infrastructure Security Agency (CISA), Department of Commerce, United States Citizenship and Immigration Services, United States Coast Guard, Department of Homeland Security (DHS), U.S. Department of Labour, and Customs and Border Protection (CBP). A

Sedgwick spokesperson stated that the incident is under investigation and clarified that the parent company's network was not impacted. The company has notified law enforcement authorities and engaged external cybersecurity specialists to assess the scope and consequences of the breach.

The Sedgwick Government Solutions breach was especially serious because attackers compromised a U.S. federal contractor that handles highly sensitive workers' compensation and medical-claims data for multiple government agencies, meaning a single intrusion exposed medical records, Social Security numbers, and employment information across several departments at once; the incident also highlighted how deeply federal systems depend on third-party processors, how attackers increasingly exploit supply-chain weaknesses instead of targeting agencies directly, and how breaches involving unchangeable personal and medical data create long-term risks far beyond a typical ransomware or corporate data leak.

Israel Advances New Cyber Law

Israel has advanced a proposed cyber law that could be taken up by various Knesset committees as early as February 2026.[4] The draft legislation was released in the last week of January and, if enacted, would mark the country's first permanent cyber law. To date, the Israel National Cyber Directorate (INCD) has functioned for nearly a decade under a patchwork of executive decisions and temporary emergency regulations issued by the prime minister or the cabinet, rather than through a dedicated statutory framework. Two of the most critical legislative challenges involve defining the circumstances and procedures under which private-sector companies and government agencies are required to notify the INCD of cyberattacks, as well as establishing when and how they must disclose such incidents to customers and suppliers.

UK–China Hold Talks on Joint Cybersecurity Forum

According to reports, British and Chinese authorities have held preliminary contacts to explore the creation of a bilateral cybersecurity forum between the two countries.[5] The proposed cyber dialogue is intended to help manage cyber threats affecting the national security of both the UK and China. Reports suggest the mechanism would enhance communication, allow for discreet exchanges, and help reduce tensions during periods of heightened cyber activity. It would also establish a direct channel between London and Beijing, enabling senior officials to discuss ongoing cyber incidents.

Pakistan-linked Cyberespionage against India

According to a threat intelligence report, a Pakistan-aligned group has launched a fresh cyber-espionage campaign targeting Indian government bodies, academic institutions, and strategic organisations.[6] The activity has been attributed to APT36, also known as Transparent Tribe, a long-running threat actor previously accused of conducting surveillance against Indian government agencies, military-linked entities, and universities. The report noted that the latest

campaign begins with spear-phishing emails containing a ZIP archive, which includes a malicious file masquerading as a PDF document. Designed to operate stealthily, the malware adapts its behaviour based on the antivirus software present on the target system. It enables remote control of infected devices, facilitates data exfiltration, and supports persistent surveillance activities such as screenshot capture, clipboard monitoring, and remote desktop access.

Hacker Steals $282M in Crypto through Social-Engineering Attack

According to reports, a hacker made off with approximately $282 million in Bitcoin and Litecoin through a social-engineering attack targeting a hardware wallet.[7] It is not yet clear whether the victim was an individual investor or an organisation. The incident reflects a broader trend observed in 2025, in which social engineering has emerged as the leading attack vector for cybercriminals. The case follows a separate incident in January 2025 when hardware wallet provider Ledger experienced a data breach after unauthorised access to user information, including names and contact details.

India File

- The Bhaskaracharya National Institute for Space Applications and Geo-informatics (BISAG-N), operating under the Ministry of Electronics and Information Technology (MeitY), has signed a memorandum of understanding with QNu Labs Pvt. Ltd. to collaborate on the development of quantum-resilient cybersecurity solutions.[8] As part of the partnership, BISAG-N's indigenous cryptographic software capabilities, including its Vedic Kavach platform, will be combined with QNu Labs' quantum hardware technologies and secure infrastructure solutions to strengthen next-generation cyber defences.

- Amid growing concerns over cybercriminal networks operating from so-called cyber slavery farms in Indochina, Indian and Cambodian officials held discussions on future cooperation and areas of mutual interest to address the issue.[9] An Indian delegation met with Cambodia's Commission for Combating Online Scam (CCOS) to explore coordinated responses to the problem. According to government data, more than 2,265 Indian nationals including software engineers had been rescued from cyber slavery operations based in Cambodia as of December 2025. Authorities noted that the exact number of Indians still trapped in the country remains unknown.

- According to reports, the Union government has informed the Supreme Court of India that it has set up a high-level inter-departmental committee to comprehensively examine all aspects of digital arrests in the country.[10] The panel is chaired by the Special Secretary (Internal Security) in the Ministry of Home Affairs and has convened three meetings so far. The most recent meeting in January included representatives from major online intermediary platforms such as Google, WhatsApp, Telegram, and Microsoft. The first meeting of the

committee was held in December, followed by a virtual session on January 2. That discussion 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, the report said.

- India is facing a growing cyber-espionage challenge after a global cybersecurity firm disclosed details of an extensive, two-year hacking campaign linked to China based APT group Evasive Panda.[11] According to the findings, the group has covertly compromised systems in India, Turkey, and China since November 2022, with some intrusions persisting for over a year. Within China, the group has targetted dissidents, ethnic minorities, and other organisations. The report states that the attackers relied on fake software updates masquerading as trusted applications to deceive users. Once installed, the malware embedded itself within legitimate system processes, enabling the threat actors to quietly exfiltrate files, record keystrokes, and run commands while largely evading detection.

[1] Government of UK, Government Cyber Action Plan, 6 January 2026, https://www.gov.uk/government/publications/government-cyber-action-plan/government-cyber-action-plan#chapter-2

[2] SGDSN, National Cybersecurity Strategy 2026-2030, https://www.sgdsn.gouv.fr/files/files/Publications/20260129_SNC%20EN_0.pdf

[3] Bleeping Computer, Sedgwick confirms breach at government contractor subsidiary, 6 January 2026, https://www.bleepingcomputer.com/news/security/sedgwick-confirms-breach-at-government-contractor-subsidiary/

[4] The Jerusalem Post, Israel moves forward with potential game-changing cyber law, 25 January 2026, https://www.jpost.com/israel-news/politics-and-diplomacy/article-884510

[5] Computer Weekly, UK and China reach out across cyber no-man's land, 21 January 2026, https://www.computerweekly.com/news/366637544/UK-and-China-reach-out-across-cyber-no-mans-land

[6] The Record, Pakistan-linked hackers target Indian government, universities in new spying campaign, 3 January 2026, https://therecord.media/pakistan-linked-hacking-group-targets-indian-orgs

[7] CoinDesk, Hacker steals $282 million crypto from a victim in social-engineering attack, 17 January 2026, https://www.coindesk.com/business/2026/01/16/hacker-steals-usd282-milion-in-hardware-wallet-social-engineering-attack

[8] PIB, BISAG-N and QNu Labs Sign MoU for collaboration and technology transfer to Strengthen India's Quantum-Resilient Cybersecurity Capabilities, 28 January 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2219756&reg=3&lang=1

[9]The Week, India Cambodia officials meet to address concerns over cyber slavery farms in Indochina, 8 January 2026, https://www.theweek.in/wire-updates/national/2026/01/08/india-cambodia-officials-meet-to-address-concerns-over-cyber-slavery-farms-in-indochina.html

[10] Scroll, Digital arrest scams: Centre tells SC it has formed multi-agency panel to tackle problem, 13 January 2026, https://scroll.in/latest/1089964/centre-tell-supreme-court-it-has-formed-multi-agency-panel-to-tackle-digital-arrests

[11] Republic, India Under Cyber Attack: Evasive Panda Spies Through Fake App Updates, Steals Data for Years, 9 January 2026, https://www.republicworld.com/tech/india-under-cyber-attack-evasive-panda-spies-through-fake-app-updates-steals-data-for-years