



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

CYBER *Digest*

October 2026

- BRICS declaration calls for ICT security and cybercrime cooperation
- IDScan confirms breach involving identity document data
- New Zealand identifies China as its most persistent cyber threat
- ShinyHunters expands exploitation of Oracle PeopleSoft vulnerabilities
- Iran-linked spyware campaign targets dissidents
- Nvidia releases AI agent security tools following AI incidents
- Australia discloses unauthorised access by OpenAI agent
- US LNG Tanker turns back after crew reports suspected cyberattack
- India File



BRICS declaration calls for ICT security and cybercrime cooperation

The BRICS New Delhi Declaration, adopted on September 12, 2026, called for stronger international cooperation on Information and Communication Technology (ICT) security as well as concerted and inclusive efforts to address the challenges stemming from and within the digital realm such as malicious software, data security, and the misuse of technologies including cybercrime, misinformation, hate-speech, disinformation and deep fakes.¹ The declaration emphasized on the need to develop a universal legal framework for responsible state behaviour in cyberspace. The declaration also encouraged states to sign and ratify the United Nations Convention against Cybercrime and recognised progress under the BRICS roadmap for ensuring security in the use of ICTs.

IDScan confirms breach involving identity document data

Identity verification company, IDScan, confirmed that an unauthorised party had accessed or copied customer information stored on its cloud platform. The disclosure followed reports that hackers were offering a large database containing scans of government issued identity documents belonging to individuals in the United States and Canada. The reports further said the database advertised on a dark web marketplace reportedly contained more than 150 million driver's license scans, along with other identity and travel documents.² IDScan confirmed ongoing

investigations and did not disclose the number of customers affected. The FBI was also reported to be investigating the incident.

New Zealand identifies China as its most persistent cyber threat

New Zealand's National Cyber Security Centre (NCSC), part of its intelligence community, assessed China to be its most persistent and capable state-backed cyber threat actor. Russia, Iran and North Korea were some other states linked with activity against government, health, education and IT sectors. The assessment covered 369 nationally significant incidents between July 2025 and June 2026, 86 of which were suspected to involve state-sponsored actors. China rejected the allegations, urging “the relevant institution in New Zealand to stop spreading lies and creating conflict”, requesting it to “do more to foster mutual understanding and trust between China and New Zealand”.³

ShinyHunters expands exploitation of Oracle PeopleSoft vulnerabilities

Google's cybersecurity unit, Mandiant, reported that the cybercrime group ShinyHunters resumed large scale exploitation of a vulnerability in Oracle PeopleSoft, after an earlier campaign between May and June 2026.⁴ According to Mandiant, the renewed activity targeted organisations that had implemented web application firewall rules but had not applied Oracle's available security update. The campaign reportedly affected dozens of systems across sectors including higher education, healthcare, government, agriculture, transportation and technology.

ShinyHunters also claimed responsibility for accessing FBI personnel information by exploiting a similar vulnerability.⁵ The breach has been compared to the 2015 records breach of the Office of Personnel Management (OPM) by China which had far-reaching consequences for the US intelligence community.⁶

Iran-linked spyware campaign targets dissidents

The United States, United Kingdom and Netherlands issued a joint cybersecurity advisory concerning an Iran-linked spyware campaign targeting dissidents, activists and journalists. The UK's National Cyber Security Centre said actors linked to Iran had used a spyware family known as “CHOSEN BRICK” in phishing campaigns conducted through messaging platforms including WhatsApp and Telegram.⁷ The advisory described attempts to obtain emails, messages and other sensitive information from targeted individuals. The disclosure was accompanied by technical information intended to assist organisations and individuals in identifying and mitigating the activity. The advisory was issued amid broader concerns about cyber-enabled surveillance and targeting of individuals outside Iran.

Nvidia releases AI agent security tools following AI incidents

Nvidia introduced a set of security tools designed to provide containment and monitoring for AI agents. The company said its technology could have prevented the high profile compromise involving the Hugging Face platform. Among the tools announced was OpenShell, intended to

isolate AI agents using CPU based controls, and Sentry, designed to terminate agents that escape their intended operating environment.⁸ Nvidia said it had worked with companies including Arm, Intel and Anthropic on compatibility and deployment. The announcement followed a series of reported incidents involving AI systems accessing external infrastructure and renewed industry discussion about securing increasingly autonomous AI agents.

Australia discloses unauthorised access by OpenAI agent

The Australian government disclosed that an OpenAI AI agent had gained unauthorised access to files on a government health data portal in June 2026.⁹ The incident came into public light only in September. According to Australian officials, the affected portal contained aggregated healthcare information rather than individual medical claims, banking details or patient medical histories. OpenAI said its investigation found no evidence that patient records had been accessed, stating that its models had taken actions that were not intended. Prime Minister Anthony Albanese tasked the country's cybersecurity agency to further investigate the incident and examine whether other government health related websites had been affected.

US LNG Tanker turns back after crew reports suspected cyberattack

The Vivit Africa LNG, carrying U.S. LNG from Louisiana's Cameron LNG terminal to Italy, reportedly experienced a systems failure while transiting the Mediterranean

and Adriatic in early September.¹⁰ The crew reported losing access to some internal control systems, prompting concerns that the disruption may have resulted from a cyberattack. The vessel did not discharge its cargo at Rovigo and subsequently sailed towards Algeciras, Spain. The Italian Coast Guard assisted the tanker after its master reported a malfunction, but said its cause had not been established. The incident remains under investigation, with no attribution to a specific actor.

India File

- External Affairs Minister S. Jaishankar signed the United Nations Convention against Cybercrime on behalf of India on 25th September 2026 in New York, on the sidelines of the 81st session of the UN General Assembly.¹¹ The Convention, formally titled the “United Nations Convention against Cybercrime, Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes,” establishes an international framework for cooperation against cybercrime and for the exchange of electronic evidence. India's signature adds the country to the states that have formally signed the Convention.
- Government of India deferred a proposal to link the Unified Payments Interface (UPI) with Alipay+, the cross-border payments platform operated by

Singapore-based Ant International.¹² The proposal raised concerns among Indian authorities regarding national security, customer-data protection, potential cyber fraud and money laundering. The proposal, submitted in January 2026, was intended initially to facilitate payments by Indian travellers through Alipay+'s merchant network in Asia, with a possible second phase allowing international visitors to use Alipay+ in India.

- Gujarat Police uncovered a network involving 5,13,847 Gmail accounts and associated credentials that investigators said had been used since 2022 to send hoax bomb threats to government offices.¹³ Two individuals were arrested in connection with the investigation. The investigation began following a bomb threat email sent to the Gujarat government on 10th September, shortly before the BRICS Summit in New Delhi. Police said some of the accounts were allegedly sold to buyers in Bangladesh, with cryptocurrency reportedly used for some payments. Investigators planned to question Google on how such a large number of accounts were created and maintained.
- Mumbai hosted APNIC 62, the Asia-Pacific Network Information Centre's regional conference, from 4-10 September. The event brought together more than 600 Internet experts, policymakers and technology professionals. Discussions covered Internet infrastructure, artificial intelligence, cybersecurity, and network

resilience.¹⁴ During the conference, NIXI and APNIC signed an MoU concerning the deployment of Internet infrastructure technologies including IPv6 and routing security. The agreement was presented as part of efforts to strengthen the security and resilience of India's Internet infrastructure. APNIC 62 also included technical workshops, policy meetings and discussions concerning the future development and security of Internet infrastructure across the Asia-Pacific region.

- India's national cybersecurity agency CERT-In issued a series of vulnerability notes during September covering widely deployed enterprise, networking and software products. Among the vulnerabilities disclosed were remote-code-execution vulnerabilities affecting Microsoft Outlook, multiple vulnerabilities in Citrix NetScaler, vulnerabilities in Check Point products, Zyxel products, Adobe products, Google Chrome, Cisco security products and other platforms. CERT-In

also issued advisories concerning vulnerabilities in Microsoft and SAP products.¹⁵

- According to Cisco's Relentless Defense Report 2026, 96% of surveyed organisations in India experienced at least one material, business-disrupting cyber incident during the preceding 12 months.¹⁶ More than one-third of these incidents involved AI enhanced attacks. The report, based on a double-blind survey of 8,000 security professionals across 30 markets, also included 1,000 respondents from India. Indian organisations recorded an average cybersecurity score of 66 out of 100, compared with a global average of 64, while 8% qualified for the report's highest-performing category. The survey also found that only 40% of Indian respondents reported cohesive functioning between security, networking and IT teams, while 44% said they spent more time collecting and correlating data across systems than addressing threats.

¹ BRICS New Delhi Declaration: Building for Resilience, Innovation, Cooperation and Sustainability, 12 September 2026, https://www.pmindia.gov.in/en/news_updates/brics-new-delhi-declaration-building-for-resilience-innovation-cooperation-and-sustainability-september-12-2026/

² ID verification giant IDScan confirms data breach with more than 150 million driver's licenses stolen, 10 September 2026, <https://techcrunch.com/2026/09/10/id-verification-giant-idscan-confirms-data-breach-with-more-than-150-million-drivers-licenses-stolen/>

³ New Zealand says China is its most persistent state-backed cyber threat, 23 September 2026, <https://www.reuters.com/world/china/new-zealand-says-china-is-its-most-persistent-state-backed-cyber-threat-2026-09-23/>

⁴ ShinyHunters hackers expanded attacks on Oracle's PeopleSoft, Google says, 26 September 2026, <https://www.reuters.com/legal/government/shinyhunters-hackers-expanded-attacks-oracles-peoplesoft-google-says-2026-09-26/>

⁵ ShinyHunters Claims FBI Hack, Demands Retraction of Threat Report, 23 September 2026, <https://www.securityweek.com/shinyhunters-claims-fbi-hack-demands-retraction-of-threat-report/>

-
- ⁶ ShinyHunters Claims FBI Job Portal Breach, Demands PSA Takedown, 24 September 2026, <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/september/fbi-data-breach>
- ⁷ Iranian cyber targeting of dissidents, activists and journalists, 15 September 2026, <https://www.ncsc.gov.uk/news/iranian-cyber-targeting-of-dissidents-activists-and-journalists>
- ⁸ Nvidia unveils security platform to stop AI agents from going rogue, 29 September 2026, <https://apnews.com/article/nvidia-ai-agent-artificial-intelligence-safety-3c4d7c1cfde82851c0577d1fa29b8621>
- ⁹ Rogue OpenAI agent 'infiltrated' Australian government website in world first, 24 September 2026, <https://www.bbc.com/news/articles/c6vgv0333dppo>
- ¹⁰ LNG Tanker Carrying US Cargo To Europe Turns Back After Crew Reports Suspected Cyberattack, 19 September 2026, <https://www.marineinsight.com/lng-tanker-carrying-us-cargo-to-europe-turns-back-after-crew-reports-suspected-cyberattack/>
- ¹¹ India Just Signed the World's First Global Cybercrime Treaty: A Global Rulebook for a Borderless Crime, 26 September 2026, <https://cyberpeace.org/resources/blogs/india-just-signed-the-worlds-first-global-cybercrime-treaty-a-global-rulebook-for-a-borderless-crime>
- ¹² Govt stalls Alipay+ tie-up over data security concerns, 4 September 2026, <https://economictimes.indiatimes.com/markets/stocks/news/govt-stalls-alipay-tie-up-over-data-security-concerns/articleshow/133749194.cms?from=mdr>
- ¹³ Indian police to query Google over 500,000 fake Gmail IDs linked to bomb hoax, 15 September 2026, <https://www.reuters.com/world/indian-police-query-google-over-500000-fake-gmail-ids-linked-bomb-hoax-2026-09-15/>
- ¹⁴ APNIC 62 Hosted by MeitY's NIXI Brings Global Internet Community Together in Mumbai, 7 September 2026, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2307289®=48&lang=2>
- ¹⁵ Vulnerability Notes, September 2026, <https://www.cert-in.org.in/s2cMainServlet?pageid=VLNLIST02>
- ¹⁶ 96% Indian firms hit by cyber incidents in past year; internal silos major hurdle: Cisco report, 30 September 2026, <https://economictimes.indiatimes.com/tech/technology/96-indian-firms-hit-by-cyber-incidents-in-past-year-internal-silos-major-hurdle-cisco-report/articleshow/134594871.cms?from=mdr>