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

# CYBER *Digest*

**January 2023**

- **Israeli audit highlights lacunae in cybersecurity measures**
- **Cyber domain focus in new Japanese NSS**
- **AIIMs servers restored after ransomware attack**
- **US increases allocation for cyber in defence budget**
- **Brazil accedes to the Budapest Convention on Cybercrime**
- **UK to make cyber incident reporting mandatory for MSPs**
- **India file**

## Israeli audit highlights lacunae in cybersecurity measures

In its latest audit, the office of the State Comptroller and Ombudsman of Israel has highlighted "significant gaps" in the military's cyberdefenses including vulnerabilities in its biometric database that contains hundreds of thousands of dental records, fingerprints and blood samples of current and former Israeli soldiers. The army has been faulted for adopting "mid-level" security of its databases, and not carrying out regular risk assessments or penetration tests to detect vulnerabilities since the establishment of the databases in 2005. Records from compromised databases pose a threat to national security since they could be used for impersonation of retired officers.[1]

Earlier in 2022, the Comptroller's office had highlighted vulnerabilities in Israel's electric and health network infrastructure, warning that the disconnect between the electricity provider and the Israel National Cyber Directorate (INCD) and method of reporting attacks has not been settled, giving rise to confusion over emergency reporting of incidents.[2]

## Cyber domain focus in new Japanese NSS

Japan released its new National Security Strategy on 16 December 2022 along with an updated National Defense Strategy (NDS) and the Defense Buildup Program (DBP). The three documents have a major focus on the cyber domain. Among the major provisions of the strategy are the inclusion of an active cyber defense posture, with the NSS stating that "For serious cyberattacks that pose security concerns against the Government, critical infrastructures, and others, the Government will be given the necessary authorities that allow it to penetrate and neutralize attacker's servers and others in advance to the extent possible." Necessary legislation which currently prohibit envisaged self-defence measures would also be modified to allow for these new actions. The National Center for Incident readiness and Strategy for Cybersecurity (NISC) in the Cabinet office will be reorganised to take charge of national cyber defence in "a centralised manner". The changes will also allow the government to defend private-sector infrastructures, such as power grids and financial networks.[3]

The accompanying National Defence Strategy sets out more specific goals and timelines. According to this document "by FY2027, MOD/SDF will establish a cybersecurity posture to secure command and control capabilities and high-priority equipment systems even under cyberattacks and to support cyber defense of the defense industry" and by 2032, the MOD/SDF would have established "a cybersecurity posture to secure command and control capabilities, force projection capabilities and operational bases to perform its missions even under cyberattacks, while reinforcing its posture to support cybersecurity of entities other than the SDF."[4] In terms of numbers, the battalion-strength Cyber Defense Command, established in 2021 with a staff of around 900, is expected to acquire division level strength of 20,000 by 2027.

## AIIMs servers restored after ransomware attack

Three weeks after the ransomware attack that paralysed medical services at the All India Institute of Medical Sciences and its affiliated networks, it was reported that most of the network had been restored even as scrubbing operations were still going on. The Minister of State in the Ministry of Electronics and Information Security (MEITY) informed the Rajya Sabha that 5 servers of AIIMS were affected and approximately 1.3 Tera Bytes of data was encrypted.[5] With increasing cyber attacks on government networks, existing

Standard Operating Procedures (SOPs) are to be more strictly enforced along with the possibility of disciplinary action against erring employees. [6] Most ransomware attacks take place because basic cyber hygiene measures such as switching off computers, signing out of emails, and updating passwords are followed haphazardly.

Though the cost of this attack is yet to be estimated, the cost of a similar attack on the Irish Health Service in 2021 was estimated recently to have crossed 80 million euros. That cyber-attack was reportedly caused by a malicious Microsoft Excel file delivered via a phishing email.

Healthcare presents a tempting target for ransomware actors given the criticality of the sector, the data rich repositories that are ripe for the taking and the enormous attack surface which make them difficult to defend against such attacks.

## US increases allocation for cyber in defence budget

The US National Defense Authorization Act (NDAA), signed into law by President Joe Biden on 23 December 2022 provides much by way of funding, authorisation and force structure review for the US military's cyber-related activities.

The Act authorises Cyber Command to carry out operations with presidential approval in "foreign cyberspace" if the president determines that there is "an active, systemic and ongoing campaign of attacks in cyberspace by a foreign power" against the U.S. government or critical infrastructure. [7] The Act allocates $44 million to Cyber Command to augment its so-called "hunt forward" missions, part of the command's strategy for "persistent engagement," defined as the need to constantly and speedily interact with adversaries in cyberspace and a further $166 million for the Cyber Mission Force. The NDAA also authorizes an increase of $56.4 million for Cybercom's Joint Cyber Warfighting Architecture (JCWA) development.[8]

Other notable provisions in the 2023 NDAA are the provisions for the creation of a Department of Defense Cyber and Digital Service Academy, where the DoD will provide scholarships to students who take courses of study related to cybersecurity for a period of no more than five years. In return, students will have to work for the same amount of time with the DoD on graduation.[9]

The NDAA also establishes a pilot program to allow the Secretary of Defense to share cyber capabilities with operational foreign partners with a list of countries suitable for cyber capabilities sharing to be drawn up by the Secretaries of Defense and State. The term 'cyber capability' as per the NDAA "means a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace"

Another area of focus is Artificial Intelligence (AI). The NDAA has new inclusions for strengthening the nation's cyber defences through AI. The legislation has directed the relevant principals in the US military to jointly develop a 5-year roadmap for adoption of AI systems and assessment of vulnerabilities posed by the use of AI in cyberspace operations.

## Brazil accedes to the Budapest Convention on Cybercrime

Brazil has become the 68th country to sign an instrument of accession to the Budapest Convention on Cybercrime during the 27th Plenary of the Cybercrime Convention Committee (T-CY) in Strasbourg, France, almost a year after it was passed by the Congress of Brazil. [10] Brazil had hitherto refused to sign the Convention, even though it

was in broad agreement with its principles, on the basis that it was not involved with the drafting process and because it felt that the Convention was biased towards Western priorities. The legislative process was marred by much opposition by digital activists and civil society groups who felt the government of Jair Bolsonaro was rushing through the process without adequate consultation.[11]

At the same plenary, six States, Croatia, Moldova, Slovenia, Sri Lanka, Ukraine and the United Kingdom also signed the Second Protocol to the Budapest Convention bringing the total to 24. The protocol is expected to enhance trans-national access for law enforcement agencies with Article 7 of the protocol allowing law enforcement in one country to directly request service providers in another country to turn over user data and identify subscribers. At least 5 member states have to ratify the additional protocol for it to come into effect.

## UK to make cyber incident reporting mandatory for MSPs

The UK government has announced proposals to introduce mandatory incident reporting requirements for managed service providers (MSPs). Going forward, MSPs will be required to disclose cyber incidents and have minimum security requirements in place with potential fines up to £17 million ($20 million) for non-compliance. While hitherto, the focus was largely on critical infrastructure, the proposed legislation takes into account the fact that in many instances, the critical infrastructure is managed by third-party services which have been out of the ambit of legislation.[12]

MSPs globally are a $200 billion segment of IT services and over 38 percent of businesses use an MSP to manage and control over their IT needs. This makes them "an attractive and high value target for malicious threat actors and can be used as staging points through which threat actors can compromise the clients of those managed services." Attacks on MSPs came to the fore in 2021 when VSA (Virtual System Administrator) software developed by Kaseya, an infrastructure provider to MSPs, was compromised, affecting up to 1,500 businesses in more than a dozen countries that were served by MSPs using the Kaseya software.[13] While supply chain insecurities are traditionally associated with hardware, software is an equally weak point.

## India file

- Microsoft has traced many critical infrastructure attacks in India to a web server discontinued in 2005, including at least 7 electricity load dispatch centres. The vulnerability in this web server was used to download malware which then attempted to run shell commands.[14]
- 30,000,000 Indian railway customer records up for sale on the dark web. The data consists of various personal identifiable information including name, email, phone number, and gender. It is not clear where the data was obtained from.[15]
- The Inter-sessional meeting of the new Open Ended Working Group (OEWG), established pursuant to General Assembly resolution 75/240, on security of and in the use of Information and Communications Technologies 2021-2025 was held at New York from 5-9 December 2022. India, in its interventions underlined the importance of capacity building and action-oriented approach to concrete deliverables during the OEWG mandate.

[1] The Times of Israel , IDF cybersecurity failures could lead to stolen identities, warns state comptroller at https://www.timesofisrael.com/idf-cybersecurity-failures-could-lead-to-stolen-identities-warns-state-comptroller

[2] The Jerusalem Post , Hackers could hit Israel's power grid, State Comptroller warns at https://www.jpost.com/israel-news/article-700786

[3] Government of Japan, National Security Strategy 2022 at https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf

[4] Government of Japan, National Defence Strategy 2022 at https://www.mod.go.jp/j/approach/agenda/guideline/strategy/pdf/strategy_en.pdf

[5] Rajya Sabha, Unstarred Question, 1223 at https://pqars.nic.in/annex/258/AU1223.pdf

[6] ET Government, Amid growing cyber threats, Centre issues new IT guidelines for key govt installations, Government News, at https://government.economictimes.indiatimes.com/news/governance/amid-growing-cyber-threats-centre-issues-new-it-guidelines-for-key-govt-installations/96196492

[7] US Congress, H.R. 7776, the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, at https://www.congress.gov/117/bills/hr7776/BILLS-117hr7776enr.pdf

[8] CSO Online, Dozens of cybersecurity efforts included in this year's US NDAA at https://www.csoonline.com/article/3683469/dozens-of-cybersecurity-efforts-included-in-this-year-s-us-ndaa.html

[9] Federal News Network, Congress greenlights expansion of Defense Department's cyber workforce at https://federalnewsnetwork.com/defense-main/2022/12/congress-greenlights-expansion-of-defense-departments-cyber-workforce/

[10] Council of Europe, Brazil accedes to the Convention on Cybercrime and six States sign the new Protocol on e-evidence at https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence#

[11] Global Voices, Opacity and a lack of debate mark Brazil's ratification of the Budapest Convention at https://globalvoices.org/2022/03/25/opacity-and-a-lack-of-debate-mark-brazils-ratification-of-the-budapest-convention/

[12] UK Government, Proposal for legislation to improve the UK's cyber resilience at https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience#annex-a-examples-of-managed-services

[13] Reuters, Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says, at https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/

[14] The Record, Microsoft attributes alleged Chinese attack on Indian power grid to 'Boa' IoT vulnerability at Microsoft attributes alleged Chinese attack on Indian power grid to 'Boa' IoT vulnerability - The Record from Recorded Future News

[15] Moneycontrol, Indian Railways data breach: 30 million user records up for sale at Indian Railways data breach: 30 million user records up for sale (moneycontrol.com)