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

CYBER *Digest*

March 2023

- **UK proposes banning of "bespoke" encrypted phones**
- **G20 Digital Economy Working Group meeting held in Lucknow**
- **New measures in Australia for critical infrastructure**
- **NCSC calls for private sector to invest in their cybersecurity**
- **Reports present insights on Russia-Ukraine cyberconflict**
- **Cyber Diplomacy Round-up**
- **India File**

UK proposes banning of "bespoke" encrypted phones

The UK Home Office has proposed making the sale and possession of certain encrypted phones illegal.[1] The proposal says that the provisions will not apply to commercially available mobile phones nor encrypted messaging apps available but only to "bespoke devices" used to facilitate organized crime. Such devices modified especially for criminal enterprises come with all trackability removed including microphone, camera and GPS. The proposal has been put out for public discussion till 21 March. [2]

As it were, encrypted communication apps such as WhatsApp and Signal are already up in arms against the UK's proposed Online Safety Bill which calls for these apps to remove illegal content from their platforms, whether communicated publicly or privately repeated. This would necessitate the removal of end-to-end encryption. Both Signal and WhatsApp have indicated that they will stop operating in the UK if the bill is passed. [3]

G20 Digital Economy Working Group meeting held in Lucknow

A 3-day long meeting of the Digital Economy Working Group of the G20 under India's presidency was held in Lucknow from February 13-15.[4] Speaking in the inaugural session, electronics and IT minister Ashwini Vaishnaw explained how the government had leveraged information technology to deliver services to citizens, giving the examples of UPI for digital inclusion and COWIN for vaccine delivery. "Today UPI is transacting over USD 1.5 trillion annually and has an average settlement time of just 2 seconds," he noted.[5] However, there is still a long way to go to mitigate cyber attacks and economic frauds.

Over 700 participants were present for the various sessions on Digital Public Infrastructure, Cybersecurity Solutions for MSMEs, Sustainable Development Goals, Geo-Spatial Technologies, and Cybersecurity and Digital Skilling in the Digital Economy. Presentations were made by various country delegations, government agencies, private companies as well as start-ups showcasing their initiatives.[6]

New measures in Australia for critical infrastructure

Australia unveiled its risk management rules for critical infrastructure and essential services as part of the security measures carried out in accordance with the security of critical infrastructure act of 2018.[7] The critical infrastructure risk management program provides for annual reporting requirements, compliance and regulatory rules, and mandatory cyber incident reporting, among other measures. [8]

Australia has also launched its Critical Infrastructure Resilience Strategy for protecting essential services, including electricity, water, healthcare, and groceries.[9] The road map under the strategy envisages risk based and resilient approaches through regulatory frameworks and industry-government collaboration. Companies have been given and period of six months to adopt a return risk management plan and another 12 months to achieve compliance.[10]

NCSC calls for private sector to invest in their cybersecurity

Speaking at the 17th India Digital Summit (IDS), Lt Gen (Retd.) Dr. Rajesh Pant, National Cybersecurity Coordinator (NCSC), said that enterprises should invest more than 10% of information technology assets in cybersecurity without any

compromise.[11] He noted that the ransomware actors had become very sophisticated in every aspect of the criminal enterprise from pinpointing which companies had cyber insurance, to using the various cloud services to mask their tracks. The government has created a national counter ransomware task force under Ministry of Home Affairs. He said that the National Cybercrime Reporting portal (www.cybercrime.gov.in) was receiving over 3500 complaints a day. The NCIIPC, with over 600 people had responsibility over the critical information infrastructure, including in the sectors of power, telecom, health, and transportation. Of these, two sectors, power and telecom had been identified as super-critical and subject to more attention. Within the power sector, Security Operations Centres (SOCs) had been put in place for Power Generation, transmission and grid operations. Chief Information Security Officers (CISOs) have also been appointed.

On the administrative and legislative front, the National Cybersecurity Strategy, created by a Taskforce headed by the NCSC with public inputs, is before the Union Cabinet. It is based on the principles of common but differentiated responsibilities. Its publication, expected in the near future, will not be a moment too soon since attacks are increasing in complexity and scale. Recent attacks have brought organisations and companies in crucial sectors to a standstill. These include the ransomware attacks on Oil India, the Nagpur based Solar Group, and Tata Power. CERT-in recorded over 14 lakhs attacks in 2022.

Among the other legislation in various stages of the systems are the Personal Data Protection Bill, the Digital India Act (superseding the IT Act on 2000) and the Telecom Bill.[12]

Reports present insights on Russia-Ukraine cyberconflict

The beginning of the year has seen a steady trickle of annual reports looking back at 2022 and highlighting the major trends seen over the previous year. This year, there is an additional raft of reports focussing on the cyber aspects of the conflict in Ukraine as they have played out over the year. In its report, *Fog of War: How the Ukraine conflict transformed the Cyber Threat Landscape*, the Google Threat Analysis Group brings out its findings and insights on state-sponsored actors, information operations and the cybercriminal ecosystem.[13] It notes that the respective agencies have to "balance competing priorities of access, collection and disruption". The East European criminal actors also splintered over political allegiances with long-term implications for this well-established ecosystem. Even though attacks on infrastructure outside the active conflict zone were less than expected, this was expected to increase as other countries increased material support and assistance to Ukraine.

The Aspens Institute Report titled *The Cyber Defense Assistance Imperative – Lessons from Ukraine* says that the abiding lesson from the conflict is that the ability to deliver cyber defence assistance "must be a key national security capability."[14] Unlike other issues like counter terrorism and non-proliferation, the private sector is indispensable to its delivery and success. Even though the assistance to Ukraine was delivered on the fly, an institutional mechanism has to be set in place for future exigencies.

Cyber Diplomacy Round-up

- The Second India-Netherlands Cyber Dialogue, co-chaired by Ms. Muanpuii

Saiawi, Joint Secretary (Cyber Diplomacy) and Ms. Nathalle Jaarsma, Ambassador at Large for Security Policy and Cyber, Government of the Netherlands, was held on 3 February 2023 in New Delhi. Discussions at the Dialogue included strategic priorities, cyber threat assessment, next generation telecommunications (including 5G technology) capacity building (including the Indo-Dutch Cyber Security School) and cooperation in multilateral fora, and the latest developments in cyber at the United Nations. The Dialogue was held in the context of recent developments in global cyberspace. It provides both the countries a platform to discuss contemporary topics of importance in cyberspace as well as a range of issues of mutual interest, and facilitates the building of a comprehensive and deeper cyber cooperation between respective cyber agencies/departments in India and the Netherlands.

- The Ministry of External Affairs facilitated a virtual meeting between Nigerian and Indian Law Enforcement Agencies (LEAs) on 7 February 2023 to discuss various issues, including WhatsApp impersonation, malware on mobile etc. at the request of I4C, Ministry of Home Affairs. Manager, Nigerian CERT led the Nigerian side during the meeting.
- The first experts meeting to negotiate the "draft Statement of Head of State of SCO Member Statement on Digital Transformation" was held online on 20 February 2023.
- MEA participated in meetings of the Working Group on Ransomware Cooperation and Diplomacy, the Working Group on Ransomware Awareness and Capacity Building, and the National Counter Ransomware Task Force (NCRTF) established by Ministry of Home Affairs.

India File

- A survey of more than Indian 1,300 business leaders by Kaspersky threw up some interesting insights. According to the survey, Indian companies are yet to streamline communication between their IT teams and other parts of the company including the C-suite. 80% of Indian companies experienced a cybersecurity incident due to poor communication channels with their IT teams, resulting in not just project delays, but also friction with the IT team and doubts over their IT skills, affecting overall work performance. [15]
- KAVACH-2023, a national level hackathon, was launched to identify innovative ideas and technological solutions for addressing the cyber security and cybercrime challenges of the 21st century. Jointly conducted by the Ministry of Education, the All India Council for Technical Education (AICTE), Bureau of Police Research and Development (BPR&D, MHA) and Indian Cyber Crime Coordination Centre (I4C, MHA), the event will be conducted in two phases. In the first phase, problem statements on fake news, social media, dark web, women safety, phishing detection, video analytics and CCTV, obscene content detection, spam alert, malware analysis, and digital forensics, would be given. In the second phase, participants are expected to come up with digital solutions for problem statements using artificial intelligence, machine learning, deep learning, augmented reality, and virtual reality. The grand finale to be held from July 12-14 would be a 36-hour-long event. Winning teams will be awarded prize money worth Rs 20 lakh.[16]

[1] *Vice*, UK Proposes Making the Sale and Possession of Encrypted Phones Illegal, 8 February 2023, https://www.vice.com/en/article/z34p49/uk-proposes-making-sale-possession-of-encrypted-phones-illegal-encrochat-sky

[2] UK Government, *Two legislative measures to improve the law enforcement response to serious and organised crime: Government consultation* , https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1137729/2023_SOC_Measures_Consultation_Document_-_Final.pdf

[3] *The Register*, Signal says it'll shut down in UK if Online Safety Bill approved, 25 February 2023, https://www.theregister.com/2023/02/25/signal_uk_online_safety_bill/

[4] *Press Information Bureau*, India , First day of the First Digital Economy Working Group meeting in Lucknow takes off, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1898943

[5] *Times of India*, Govt prevented lakhs of cyber attacks: Uttar Pradesh minister Ashwini Vaishnaw https://timesofindia.indiatimes.com/city/lucknow/govt-prevented-lakhs-of-cyber-attacks-min/articleshow/97896524.cms

[6] India Stack, *First Meeting of G20 Digital Economy Working Group (13-15 Feb 2023)* https://www.indiastack.global/g20-dewg

[7] Australian Government, *Federal Record of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*, https://www.legislation.gov.au/Details/F2023L00112

[8] Australian Government, *Cyber and Security Infrastructure Centre, Critical Infrastructure: Regulatory Obligations*, https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure/regulatory-obligations

[9] *Bank Infosecurity*, Australia Unveils Game Plan to Guard Critical Infrastructure,21 February 2023, https://www.bankinfosecurity.com/australia-unveils-game-plan-to-guard-critical-infrastructure-a-21276

[10] Australian Government, *Cyber and Infrastructure Security Centre, Critical Infrastructure Resilience Strategy*, https://www.cisc.gov.au/resources-contact-information-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf

[11] *The Hindu*, Firms should invest over 10% of IT assets in cyber security: Rajesh Pant, 21 February 2023, https://www.thehindu.com/business/firms-should-invest-over-10-of-it-assets-in-cyber-security-rajesh-pant/article66533752.ece

[12] YouTube, *Lt Gen (Retd.) Dr. Rajesh Pant live at #17IDS on Cybersecurity of a Nation*, https://www.youtube.com/watch?v=lvKZsGfDWUs

[13] Google, *Fog of War: How the Ukraine conflict transformed the Cyber Threat Landscape, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf*, 16 February 2023

[14] The Aspen Institute, *The Cyber Defense Assistance Imperative – Lessons from Ukraine*, 16 February 2023, https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf

[15] *The Hindu*, 80% of Indian companies hit by cybersecurity incidents after miscommunication with IT team: Kaspersky report, 21 February 2023, https://www.thehindu.com/sci-tech/technology/80-indian-companies-hit-cybersecurity-incidents-miscommunication-it-team-kaspersky-report/article66535520.ece

[16] *Press Information Bureau*, AICTE and BPRD Jointly Launch KAVACH-2023, a National Level Hackathon to tackle cyber threats and provide effective solutions, 16 February 2023, https://pib.gov.in/PressReleseDetail.aspx?PRID=1899836