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

CYBER *Digest*

April 2023

- Country Scans: US, UK and China
- Microsoft updates Russia-Ukraine hybrid war report
- Russian government bans foreign messaging apps
- Belgium and New Zealand ban TikTok on government devices
- Austrian Data Protection Authority rules against META
- India File

Country Scans

United States

1. The Biden administration published its long-awaited National Cybersecurity Strategy to ensure the full benefits of a safe and secure digital ecosystem for all Americans.[1] The document sets out to address threats emanating from future-generation technologies and secure a safe digital future for Americans. The document also promises the US and its allies a secure, resilient, values-aligned digital ecosystem. The strategy seeks to build and enhance collaboration around five pillars:

   - Defend Critical Infrastructure
   - Disrupt and Dismantle Threat Actors
   - Shape Market Forces to Drive Security and Resilience
   - Invest in a Resilient Future
   - Forge International Partnerships to Pursue Shared Goals

   The strategy is also part of a more significant effort by the Biden administration to strengthen governance in cyberspace. This included efforts to increase the accountability of tech companies and boost privacy protections for users.[2]

2. The US Department of Defence has introduced a new cyber workforce strategy to ease entry, exit, and re-entry into its cyber workforce.[3] The underlying reason behind the strategy is to strengthen talent acquisition and retention amid the growing global cyber talent shortage. Through this, the Defence Department is also seeking to establish a system enabling members of its cyber workforce to leave for the private sector and return with newly acquired skills.

3. The Cybersecurity and Infrastructure Security Agency (CISA) has established the Ransomware Vulnerability Warning Pilot (RVWP) as authorized by the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022.[4] The reason behind the program is the growing threat of ransomware attacks against organizations and public entities. Under its remit, RVWP will warn critical infrastructure entities about the vulnerabilities, enabling mitigation before a ransomware incident occurs. Earlier, in May 2022, CISA announced the formation of a joint ransomware task force, as required under the same Act.[5]

4. A group of US Senators asked CISA to examine the consumer drones built by Shenzhen DJI Innovation Technology, a company they accuse of having links to China’s government.[6] The call for an inquiry is amidst an expansion in commercial drones across the US, from food delivery to emergency services. The senators also noted that CISA published its own alert in 2019, raising concerns about all drones manufactured in China. Reuters reported in 2021 that DJI controlled almost 90% of the consumer market in North America and over 70% of the industrial market.[7]

5. The Military Cyber Professionals (MCPA), a US-based association of current and former digital security leaders, urged lawmakers to establish a US Cyber Force in this year’s National Defense Authorization Act.[8] In their memorandum, the association noted that highly contested cyberspace is the only domain of conflict without an aligned service.[9]

6. The White House has issued an executive order barring federal government agency from using commercial spyware products that pose a national security risk or have

been misused by foreign actors to enable human rights abuses worldwide.[10] The order noted that foreign governments worldwide use surveillance tools and have not been limited to authoritarian regimes. The directive also highlighted the growing incidents of US government personnel being targeted by commercial spyware and untrustworthy commercial vendors and how that poses a significant risk to security.

United Kingdom

1. The UK government has announced the creation of the National Protective Security Authority (NPSA) to help businesses and organizations defend themselves against national security threats.[11] The new body has also absorbed the responsibilities of the Centre for the Protection of National Infrastructure but with a broader remit. The NPSA will closely work with partners such as the National Cyber Security Centre and the National Counter Terrorism Security Office to provide holistic security advice to policy makers.

2. The UK government has published a cybersecurity strategy for the healthcare and social care sector that sets out to protect National Health Service (NHS) from cyberattacks.[12] The cyber strategy sets out key ways to build cyber resilience in health care by 2030 and will protect health and social care functions services, which the whole nation depends on. The vision includes five key pillars to minimize the risk of cyber-attacks and improve response and recovery following incidents across health and social care systems.

3. In a major step to counter cybercriminal activities, the UK's National Crime Agency (NCA) has revealed that it created multiple fake DDoS-for-hire-service websites to identify cybercriminals who utilize these platforms to target organizations.[13] The NCA used these fake websites to collect information on those registered to use these services. The NCA noted that the underlying reason behind such initiatives is to undermine trust in criminal markets and stop DDoS attacks at their source.

China

1. China's State Council Information Office released a white paper titled "China Law-Based Cyberspace Governance in the New Era".[14] The document stressed the importance of rule of law in cyberspace as an important tool of digital governance and also as a marker of progress in the digital domain. The white paper also expounded role of international cooperation in cyberspace.

2. Researchers with Google have discovered China-backed cyber operations that have hit private and government networks in the US. The analysts have discovered hacks of systems that are not usually the target of cyber-espionage operations. These breaches represent new level of ingenuity and sophistication from China.[15]

Microsoft updates Russia-Ukraine hybrid war report

Microsoft updated its analysis on the Russian hybrid warfare in Ukraine. The report concludes that Russia's cyber and influence operations have largely failed against a resilient Ukrainian population.[16] The document examines Russia's propaganda ecosystem targeting Ukraine including Russian intelligence-linked media and how its cyber-influence operations have focused on undermining Kyiv's foreign and domestic support. Russia is also seen to have paired kinetic operations with cyber-operations targeting sectors such as energy, telecommunications, health care, transportation and other essential infrastructures.

Russian government bans foreign messaging apps

The Russian government has banned the use of foreign messaging applications in the Russian government and state agencies.[17] The banned services mentioned by Roskomnadzor (Russia's internet watchdog agency) include the following: Discord, Microsoft Teams, Skype for Business, Snapchat, Telegram, Threema, Viber, WhatsApp, WeChat. The list of banned applications does not include Zoom (video conferencing) and Signal (encrypted messaging service).[18]

Some reports say also say that Russian officials close to the presidential office were asked to ditch their iPhones by the end of March amid growing information-security concerns.[19] The directive asked officials to replace their iPhones with phones built on other smartphone software developed by Chinese and Russian companies.

Belgium and New Zealand ban TikTok on government devices

The Belgium government has formally banned the use of the TikTok app on government devices, citing security risks posed by the application.[20] The New York Times reported that many countries had expressed concerns that TikTok, which is owned by the Chinese ByteDance, may endanger sensitive user data.[21] Amid mounting international security concerns surrounding the app, New Zealand's parliament also decided to block the application from all parliamentary devices.[22] Going a step further, the French government banned all recreational apps from government-managed devices.[23]

Austrian Data Protection Authority rules against Meta

The Austrian Data Protection Authority has ruled that Facebook's use of its tracking pixel directly violates the GDPR.[24] Reportedly the personal data was transferred to the US, where the information was at risk from government surveillance. The finding is the result of complaints filed by the European privacy rights group NOYB. However, the data protection authority issued no penalty in the ruling.

India File

1. According to Check Point Software Technologies, India reported 1,787 cyber attacks a week on average in an organization in the last six months, compared to the global average of 983.[25] The most attacked segment in India is the healthcare industry, followed by the defence and education sectors.

2. According to an assessment by Cisco, just 24% of organizations surveyed in India have the mature level of readiness required to be resilient against emerging cybersecurity threats.[26] About 38% of companies in India fall into the beginner or formative stages; however, organizations in India are faring better than the global average. The report also said that 80% of around 1000 respondents in India had reported a cyber incident in the last 12 months.

3. Drug major Sun Pharmaceuticals reported that the company faced a cyber-incident perpetrated by a ransomware group.[27] The company reported to have taken appropriate steps to contain the damage and have isolated the impacted assets along with initiating the recovery process. The company also said that business operations have been impacted following the incident and may also have an impact on its revenues.

4. The Securities and Exchange Board of India (SEBI) have announced a cybersecurity framework for all portfolio managers.[28] The circular said that the new policy will come into force from October 1, 2023 and will ask portfolio managers to report all cyber-attacks and breaches experienced by them within 6 hours of detecting such incidents. The portfolio managers have also been asked to define the responsibilities of its employees, outsourced staff, and employees of vendors and other entities, who may have access to their network. This follows close on the heels of an advisory put out to all regulated entities, including financial sector organisations, stock exchanges, depositories, mutual funds and other financial entities, in February 2023 asking them to provide compliance of the advisory along with their cybersecurity audit report.[29]

Cyber diplomacy Round-up

1. The Fourth Substantive Session of UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) 2021-2025 was held in New York from 06-10 March 2023.

2. A number of Experts meeting to negotiate the 'Draft Statement of Heads of State of SCO Member Statement on Cooperation in Digital Transformation' was held online during the month.

5. The Asia-regional Multi-Stakeholder Consultations to elaborate on United Nations Global Digital Compact (GDC) was organized from 21-22 March 2023 in New Delhi. The agenda of the meeting was to discuss on the role of Digital Public Infrastructure (DPI) in the GDC to achieve SDG 2030 Agenda of ensuring inclusive, open, accessible, safe and affordable digital technologies and digital infrastructure. Around 60 participants, including officials and think tanks from Asian countries attended the two-day event.

[1] The White House, Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy, 2 March 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[2] World Economic Forum, The US has announced its National Cybersecurity Strategy: Here's what you need to know, 9 March 2023, https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/

[3] SC Media, New cyber workforce strategy released by Defense Department, 13 March 2023, https://www.scmagazine.com/brief/careers/new-cyber-workforce-strategy-released-by-defense-department

[4] Cybersecurity & Infrastructure Security Agency (CISA), CISA Establishes Ransomware Vulnerability Warning Pilot Program, 13 March 2023, https://www.cisa.gov/news-events/news/cisa-establishes-ransomware-vulnerability-warning-pilot-program

[5] Security Boulevard, CISA Announces Joint Ransomware Task Force, 25 May 2022, https://securityboulevard.com/2022/05/cisa-announces-joint-ransomware-task-force/

[6] The Record, Senators call on CISA to examine cybersecurity risks of Chinese consumer drones, 16 March 2023, https://therecord.media/senate-drone-cisa-china-warner-blackburn

[7] Reuters, Game of drones: Chinese giant DJI hit by U.S. tensions, staff defections, 8 March 2021, https://www.reuters.com/article/us-usa-china-tech-dji-insight/game-of-drones-chinese-giant-dji-hit-by-u-s-tensions-staff-defections-idUSKBN2AZ0PV

[8] The Record, US military needs 7th branch just for cyber, current and former leaders say, 27 March 2023, https://therecord.media/us-cyber-force-creation-proposed-mcpa

[9] Military Cyber Professionals Association (MCPA), The MCPA calls for the creation of a US Cyber Force, 26 March 2023, https://public.milcyber.org/legislation

[10] The White House, President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security, 27 March 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security

[11] GOV.UK, National Protective Security Authority begins work, 13 March 2023, https://homeofficemedia.blog.gov.uk/2023/03/13/national-protective-security-authority/

[12] GOV.UK, Government sets out strategy to protect NHS from cyber-attacks, 22 March 2023, https://www.gov.uk/government/news/government-sets-out-strategy-to-protect-nhs-from-cyber-attacks

[13] Bleeping Computer, UK creates fake DDoS-for-hire sites to identify cybercriminals, 24 March 2023, https://www.bleepingcomputer.com/news/security/uk-creates-fake-ddos-for-hire-sites-to-identify-cybercriminals/

[14] China Daily, China issues white paper on law-based cyberspace governance in new era, 16 March 2023, https://www.chinadaily.com.cn/a/202303/16/WS6412812ca31057c47ebb4d0b.html

[15] Wall Street Journal, Wave of Stealthy China Cyberattacks Hits U.S., Private Networks, Google Says, 16 March 2023, https://www.wsj.com/articles/wave-of-stealthy-china-cyberattacks-hits-u-s-private-networks-google-says-2f98eaed

[16] Microsoft, A Year of Russian hybrid warfare in Ukraine, 15 March 2023, https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

[17] Infosecurity, Russian Government Bans Foreign Messaging Apps, 2 March 2023, https://www.infosecurity-magazine.com/news/russian-government-bans-foreign/

[18] Bleeping Computer, Russia bans foreign messaging apps in government organizations, 1 March 2023, https://www.bleepingcomputer.com/news/security/russia-bans-foreign-messaging-apps-in-government-organizations/

[19] Business Insider, The Kremlin has reportedly told Russian officials to throw away their iPhones by the end of the month, 21 March 2023, https://www.businessinsider.in/tech/news/the-kremlin-has-reportedly-told-russian-officials-to-throw-away-their-iphones-by-the-end-of-the-month/articleshow/98831471.cms

[20] Reuters, Belgium bans TikTok from federal government work phones, 11 March 2023, https://www.reuters.com/technology/belgium-bans-tiktok-federal-government-work-phones-2023-03-10/

[21] The New York Times, Why Countries Are Trying to Ban TikTok, 27 March 2023, https://www.nytimes.com/article/tiktok-ban.html

[22] The Guardian, New Zealand to ban TikTok from government devices, 17 March 2023, https://www.theguardian.com/world/2023/mar/17/new-zealand-to-ban-tiktok-from-government-devices

[23] Techcrunch, France bans recreational apps like TikTok on government devices, 27 March 2023, https://techcrunch.com/2023/03/27/france-bans-recreational-apps-like-tiktok-on-government-devices

[24] Techcrunch, Use of Meta tracking tools found to breach EU rules on data transfers, 16 March 2023, https://techcrunch.com/2023/03/16/meta-tracking-gdpr-data-transfer-breach

[25] The Wire, India Saw Over 1,700 Cyber Attacks a Week in Last 6 Months, Double the Global Average: Report, 27 March 2023, https://thewire.in/tech/india-cyber-attacks-last-6-months

[26] Outlook, Just 24% Of Companies Surveyed In India Ready To Defend Cybersecurity Threats: Cisco Study, 21 March 2023, https://www.outlookindia.com/business/just-24-of-companies-surveyed-in-india-ready-to-defend-cybersecurity-threats-cisco-study-news-271941

[27] NDTV, Drug Major Sun Pharma Hit By Ransomware Attack: 5 Facts, 27 March 2023, https://www.ndtv.com/india-news/drug-major-sun-pharma-hit-by-ransomware-attack-5-facts-3896122

[28] Outlook, SEBI Puts In Place Cybersecurity Framework For Portfolio Managers, 30 March 2023, https://www.outlookindia.com/business/sebi-puts-in-place-cybersecurity-framework-for-portfolio-managers-news-274528 https://www.outlookindia.com/business/sebi-puts-in-place-cybersecurity-framework-for-portfolio-managers-news-274528

[29] SEBI, Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices, 22 February 2023 https://www.sebi.gov.in/legal/circulars/feb-2023/advisory-for-sebi-regulated-entities-res-regarding-cybersecurity-best-practices_68334.html