



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

CYBER *Digest*

December 2021

- **PM Modi highlights cybersecurity at Sydney Dialogue**
- **US blacklists Israeli firms for use of spyware**
- **Government to move bill to regulate 'private cryptocurrencies'**
- **INTERPOL conducts operation against cybercrime entities**
- **British MI 6 head talks about the challenges of new technologies**
- **India file**



PM Modi highlights cybersecurity at Sydney Dialogue

Prime Minister Narendra Modi, while delivering the keynote address at the Sydney Dialogue on 18 November highlighted the need for democracies to work together to ensure that the fruits of the digital revolution are not misused by vested interests. He noted this was of the utmost importance since technology had become a major instrument of global competition and even though it had ushered in a new era of opportunities for progress and prosperity, it had also given rise to new risks and new forms of conflicts.

Giving a roadmap for democracies to work together, he called for a collaborative framework "to invest together in research and development in future technology; to develop trusted manufacturing base and trusted supply chains; to deepen intelligence and operational cooperation on cyber security, protect critical information infrastructure; to prevent manipulation of public opinions; to develop technical and governance standards and norms consistent with our democratic values; and, to create standards and norms for data governance and for cross-border flows that protect and secure data." ¹

US blacklists Israeli firms for use of spyware

In an unprecedented action, the US Department of Commerce has blacklisted two Israel firms and banned them from buying software components from US vendors without a license. The two companies, the NSO group and Candiru, have been accused of targeting US government officials and journalists.² While NSO had repeatedly assured the US

government that its software was configured not to hack into phone numbers starting with the US country code +001, another report highlighted that phones of US diplomats based in Uganda had been hacked using the software. Apple has also filed a lawsuit against the NSO group for using Pegasus spyware to surveil its users.

Government to move bill to regulate 'private cryptocurrencies'

The government has issued notice to introduce a bill to regulate private cryptocurrency. "The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021" also encompasses a framework for the creation of official digital currency which will be issued by the Reserve Bank of India. A study by Chainalysis shows that India is second in crypto adoption worldwide, and considering this, some industry experts believe that regulation would not be technologically feasible since crypto wallets do not require the use of local currency and hence do not come under the purview of governments. In addition, peer to peer networks are difficult to monitor as users can simply transfer money through bank accounts and exchange equivalent crypto through wallets. The chairman of the Parliamentary Standing Panel, Mr Jayant Sinha expressed the importance of balance between regulation and innovation stating that the crypto exchanges have 15 million KYC approved users with a \$6 billion investment.

INTERPOL conducts operation against cybercrime entities

In an operation coordinated by INTERPOL, law enforcement agencies from over 20 countries arrested over 1000 individuals and seized more than \$27 million worth of

illicit funds that had been collected through many types of online fraud, including romance scams, investment fraud, and money laundering. The operation was conducted over 4 months and the countries involved included Angola, Brunei, Cambodia, Colombia, China, India, Indonesia, Ireland, Japan, South Korea, Laos, Malaysia, Maldives, Philippines, Romania, Singapore, Slovenia, Spain, Thailand, and Vietnam.

A new global stop-payment mechanism, the Anti-Money Laundering Rapid Response Protocol (ARRP) was also tested out during the operation and proved to be critical to its successful completion.³

British MI 6 head talks about the challenges of new technologies

In a speech to the International Institute for Strategic Studies, the head of British intelligence agency MI 6 noted that according to some assessments, there would be more “technological progress in the next ten years than in the last century, with a disruptive impact equal to the industrial revolution.” According to him, adversaries were “pouring money into mastering artificial intelligence, quantum computing and synthetic biology.” Matching this effort could only be done in close co-operation with the private sector.

With the digital attack surface growing exponentially, one of the dilemmas faced by an intelligence agency was how to operate in an ethically complex environment as a democracy bound by rule of law.

A large part of his speech was devoted to the multiple threats from China; its use of technologies of control and surveillance which were also increasingly being

exported to other likeminded governments thereby “expanding the web of authoritarian control around the planet.”⁴

India file

- The business of government continued virtually with Ministry of External Affairs conducting the Second edition of the India-New Zealand Bilateral Cyber Dialogue being from 16-17 November 2021. The Indian delegation was led by Atul Malhari Gotsurve, Joint Secretary (Cyber Diplomacy), MEA and the New Zealand delegation was co-led by Dan Eaton, Director National Security Policy, Department of Prime Minister and Cabinet (DPMC) and Georgina Sargison, Acting Unit Manager, Emerging Security Issues, International Security and Disarmament Division, Ministry of Foreign Affairs and Trade (MFAT).
- The first meeting of the India-UK Joint Working Group on Cyber Deterrence was held on 25 November 2021. The Indian delegation was led by Atul Malhari Gotsurve, Joint Secretary (Cyber Diplomacy), Ministry of External Affairs (MEA). The UK delegation was led by Will Middleton, Cyber Director from Foreign Commonwealth Development Office (FCDO). Both sides discussed various key aspects related to cyber deterrence agreed to work closely with each other and hold regular consultations on addressing the challenges to cyber deterrence and for building effective cyber deterrence strategies.
- The Department of Telecommunications (DoT) and International Telecommunication Union (ITU)

conducted the India-ITU Joint Cyberdrill 2021 virtually from 30 November to 3 December. Over 400 participants, including those from the

critical sectors of power, insurance, finance, and telecom, as well as CERT-In and CSIRT, industry, and academia, took part in the 4-day event.

¹ PM's Keynote Address at the Sydney Dialogue, at https://www.pmindia.gov.in/en/news_updates/pms-keynote-address-at-the-sydney-dialogue/

² Israeli firm NSO Group blacklisted by the US for use of spyware at <https://edition.cnn.com/2021/11/03/tech/nso-group-us-blacklist/index.html>

³ More than 1,000 arrests and USD 27 million intercepted in massive financial crime crackdown

at <https://www.interpol.int/en/News-and-Events/News/2021/More-than-1-000-arrests-and-USD-27-million-intercepted-in-massive-financial-crime-crackdown>

⁴ C's speech to the International Institute for Strategic Studies at <https://www.gov.uk/government/speeches/cs-speech-to-the-international-institute-for-strategic-studies>