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

CYBER *Digest*

September 2021

- American businesses to spend billions to improve cybersecurity
- Cybersecurity agreements signed between US and Singapore
- WhatsApp fined 225 million euro over privacy breach
- New CII Cyber Regulations in China
- Cybersecurity discussed at Colombo Conclave
- Pakistan's National Cyber Security Policy 2021 approved
- Boost for Bangladesh in National Cyber Security Index ranking

American businesses to spend billions to improve cybersecurity

American business leaders from top companies across critical infrastructure sectors participated in a cybersecurity summit hosted by the White House on 25 August 2021.[1] The move comes at a time when widespread cyberattacks took place throughout the year targeting critical infrastructure, software companies and government networks.

Big Tech companies promised to spend billions on cybersecurity at the meeting. Apple, Amazon, IBM would also help secure the cybersecurity architecture by getting involved in various training programs and investments.

The reasons for repeated cyber-attacks were attributed to the dependence of organisations on vulnerable legacy infrastructure.[2] Nation-state actors and cybercriminals target weaknesses in software supply chains which many vendors are unable to prevent due to lack of expertise. . Extending the zero-trust security model, securing the software supply chain apart from strengthening the digital security skills of the American workforce were some of the solutions discussed.

Cybersecurity agreements signed between US and Singapore

The United States and Singapore finalised three agreements on cybersecurity to expand cooperation with respect to the financial sector, military-to-military engagement, and regional capacity-building during the US Vice President, Kamala Harris' visit to Singapore.[3]

These agreements include a bilateral MOU on Cybersecurity Cooperation between the U.S. Department of the Treasury and the Monetary Authority of Singapore which would help both the financial sectors to be more prepared for, and resilient to cyber threats in the new era. Bilateral information sharing on cyber threats to financial markets will also be facilitated as per the agreement.

The second agreement was finalised as an MOU on Cyber Cooperation between the U.S. Department of Defense and the Singapore Ministry of Defense. This would help support broad defense cooperation between the two defence organisations and also help in advanced cybersecurity information sharing and exchange of threat indicators. Combined cyber training exercises and other forms of military-to-military cooperation on cyber issues will also be facilitated.

The third agreement was a bilateral MOU between the U.S. Cybersecurity and Infrastructure Security (CISA) and the Cyber Security Agency of Singapore (CSA) to enhance exchange of information on cyber threats and defensive measures. Increased coordination between the two departments for cyber incident response and cybersecurity capacity building across Southeast Asia would be encouraged.

WhatsApp fined 225 million euro over privacy breach

WhatsApp has been fined an amount of 225 million euro by Ireland's Data Protection Commission for breach of data privacy.[4] WhatsApp has been accused of non-adherence to the European Union General Data Protection Regulation (GDPR) and lack of transparency regarding the mechanism of sharing user data with other companies like Facebook, its parent company.

The Data Protection Commission had launched a probe in December 2018 to look into the data privacy mechanisms of WhatsApp and if it "discharged its GDPR transparency obligations". WhatsApp however has claimed that the company had provided information regarding the queries made during the 2018 probe and has called the fine as "entirely disproportionate".

A number of tech companies have their regional headquarters in Ireland which include companies like Apple, Google, Facebook and Twitter. The Irish Data Protection Commission is active in ensuring that these companies adhere to the General Data Protection Rules (GDPR).

Earlier in July, the tech giant Amazon was fined a record $886.6 million euro by the Luxembourg privacy agency. The European Data Protection Board, the EU privacy watchdog, had asked the Irish agency to decide quickly regarding the pending cases involving the tech giants and also to impose appropriate fines due to noncompliance of data rules.

New CII Cyber Regulations in China

China's State Council has come up with new cybersecurity regulations for the "Critical Information Infrastructure" (CII) operators in the country. The “Regulation on Protection of Security of Critical Information Infrastructure” aims to bring tech companies in the CII category under its purview from September 1.[5]

The draft of this regulation was published in July 2017 and put up for public comment. The final version of the rules specify that the Protecting Authorities of the critical industries will have to determine who are CII operators and formulate their own rules done in coordination with the Cybersecurity Administration of China along with the Ministry of Public Security.

Some other compliance requirements for CII operators mentioned are to establish a management body to carry out cybersecurity practices, annual internal security risk assessments and purchasing "secure and reliable" network products and services. Apart from this, it also imposes special data protection and procurement rules on CII operators. An emergency response plan is to be formulated alongside regular emergency exercises.

Failure to adhere to the rules may lead to serious penalties (up to RMB 1 million or 10 times the price of the product or service procured) to the CII operators, in addition to the penalties as per their Criminal Law.

Cybersecurity discussed at Colombo Conclave

At the Deputy National Security Adviser level meeting hosted by Sri Lanka on August 4, marine safety and security, terrorism and radicalisation, trafficking and organised crime, and cybersecurity were identified as the "four pillars" of cooperation.[6] The trilateral security meeting between Sri Lanka, India and Maldives was held virtually. Bangladesh, Mauritius and Seychelles participated as Observers.

The security conclave was chaired by General LHSC Silva, Chief of Defence Staff and Commander of Army of Sri Lanka. Mr. Pankaj Saran, Deputy NSA India represented India and Maldives was represented by Aishath Nooshin Waheed, Secretary, NSA's Office.

The idea of a Colombo Security Conclave was conceived in November 2020 at the

NSA-level meeting of India, Lanka and Maldives. It mainly focuses on a closer cooperation on maritime and security matters among the three Indian Ocean countries.

The meeting discussed specific proposals for cooperation among the three countries in each of these pillars. Capacity building, joint exercises and training activities were identified as mechanisms for regional cooperation. Apart from that, the three observer states were invited to join as members in the next meet. This could further lead to greater coordination and do-operation in the four pillars identified in this meeting. [7]

Pakistan's National Cyber Security Policy 2021 approved

The federal cabinet of Pakistan approved the National Cyber Security Policy 2021 that will allow establishment of a national cyber security response framework for implementation of cybersecurity policies in the country.[8] The Cyber Governance Policy Committee would look after implementation of the policy.

With Pakistan ranking as the seventh worst cyber-secure state in the world as per the Global Strategies Index and the Global Security Index 2018 report, this is a right step in the direction of improving the cybersecurity architecture in the country.

The committee will be responsible for implementing the policy at the national level. A cyberattack on any organisation in Pakistan would be considered as an act of aggression and an attack on the national sovereignty as per the policy which would lead to all necessary and retaliatory steps to be taken. The policy supports: establishment of an internal framework in all institutions including private ones for the protection of cyber ecosystem, protection of ICT infrastructures, ensuring cybercrime monitoring, capacity building, cyber skill development and training programmes. The IT ministry will help establish active cyber defence, play the role of awareness generation and also develop cybercrime response mechanisms and frame regulations for the same.

Boost for Bangladesh in National Cyber Security Index rankings

Bangladesh ranked 38 among 160 countries in the latest iteration of the National Cyber Security Index (NCSI) brought out by the e-Governance Academy Foundation, Estonia[9]. The index is prepared on the basis of an analysis of the cyber security and digital development in the participating countries. It is a dynamic index with rankings revised several times a year based on developments in the respective countries. The Index acts as a benchmark for countries to make an assesment of their cybersecurity preparedness. The development of the National Cyber Security Index was funded by the Estonian Ministry of External Affairs.

Greece topped the index with a score of 96. The United States ranked 17 and the United Kingdom ranked 19. Singapore made it to the top 20, being the only Asian country to do so. Japan ranked 34, India ranked 39, Pakistan, 70, and China ranked 83 among the other Asian countries.

[1] Google, Microsoft plan to spend billions on cybersecurity after meeting with Biden at https://www.cnbc.com/2021/08/25/google-microsoft-plan-to-spend-billions-on-cybersecurity-after-meeting-with-biden.html

[2] https://blog.google/technology/safety-security/why-were-committing-10-billion-to-advance-cybersecurity/

[3] The White House, FACT SHEET: Strengthening the U.S.-Singapore Strategic Partnership at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/23/fact-sheet-strengthening-the-u-s-singapore-strategic-partnership/

[4] Ireland fines WhatsApp €225 million for EU privacy breach at https://www.dw.com/en/ireland-fines-whatsapp-225-million-for-eu-privacy-breach/a-59065206

[5] “Am I a CII operator?” – New regulation in China provides more clarity https://www.dataprotectionreport.com/2021/08/am-i-a-cii-operator-new-regulation-in-china-provides-more-clarity/

[6] Cybersecurity, terrorism, marine safety identified among "four pillars" of cooperation at security meeting between Lanka, India, Maldives at https://www.aninews.in/news/world/others/cybersecurity-terrorism-marine-safety-identified-among-four-pillars-of-cooperation-at-security-meeting-between-lanka-india-maldives20210806220750/

[7] HCI Colombo Press Release, DEPUTY NATIONAL SECURITY ADVISER LEVEL MEETING OF THE COLOMBO SECURITY CONCLAVE at https://www.hcicolombo.gov.in/press?id=eyJpdiI6IkYxQnp0Q09OcDB0SkZIcVRJY1wvdklBPT0iLCJ2YWx1ZSI6IlVtXC9lcU50eGJReW54ZTdPeHRLMHlBPT0iLCJtYWMiOiI3YjJkYzVhYTllOTE0OWFlMTc3YTA3Y2ZjYTZlOTg0MTU1MTg4NDUzYTMxMzBlNWQwMzI5MmM0NDZiNzc5NTNkIn0=

[8] Cabinet gives the green light to cyber security policy at https://www.dawn.com/news/1637334

[9] Bangladesh tops National Cyber Security Index among SAARC nations at https://www.tbsnews.net/bangladesh/bangladesh-tops-national-cyber-security-index-among-saarc-nations-292174