MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES

मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

January 2021

- **QUAD Tech Network Initiative**
- **MOU between Kaspersky and CERT-In**
- **Public Wi-Fi Access Network Interface gets green signal**
- **The SolarWinds cyberattack**
- **Global outage of Google services**

QUAD Tech Network Initiative

The Australian Department of Foreign Affairs and Trade (DFAT) has allocated AUD 497,000 for a QUAD Tech Network project under QUAD (Quadrilateral Security Dialogue). A notice on the government's grant website said that QTN is to be set up by DFAT's Cyber Affairs and Critical Technology Branch to support and complement the development of Australia's first Cyber and Critical Technology International Engagement Strategy (CCTIES).

The move aims at strengthening the cooperation between the QUAD countries namely- Australia, the US, Japan and India on cyber and critical technology issues. The major objective of QTN would be focussing on protecting the cyberspace including 5G networks and preventing the misuse of artificial intelligence AI mainly in Australia's interests as a liberal democracy committed to the international rules-based order.

The QTN will be managed by the Australian National University (ANU) on behalf of DFAT. It would engage researchers from partner think tanks and universities of QUAD countries to promote technology –exchange. It will also provide the opportunity for Cyber Affairs and Critical Technology Branch to leverage expertise through the facilitation of private video teleconference calls. [1]

The Australian foreign affairs minister, Marise Payne, in a technology conference hosted by the Indian partner of QTN, Observer Research Foundation, urged member countries and other like-minded countries, to work together to build "a digital Indo-Pacific that is free, open and trusted" and adapt to technological change in a transparent way.[2]

QUAD is an effective example of multilateralism based on shared interests and values of like-minded countries in the Indo-Pacific region. Cooperation in the digital domain would go a long way in efforts to secure the digital security architecture of the member countries including that of India.

MOU signed between Kaspersky and CERT-In

Kaspersky has signed a memorandum of understanding (MoU) with the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India, for collaboration in the area of cybersecurity.

With increased digitisation especially during the pandemic, it is important to create a robust, safe and secure information infrastructure in the country. The MoU will facilitate cooperation between cyber-security experts from kaspersky and the government to help achieve this goal. The primary role of CERT-in has been to raise security awareness among the Indian cyber community and provide technical assistance to them. Kaspersky's expertise and access to global data on evolving threat landscapes will support this role.

The MOU also seeks to share data feeds and intelligence between the two entities in areas such as cyber security incident reporting, incident analysis and response, cyber security audit, and malware analysis.[3] It also intends to enhance the general public's trust on digital systems by devising appropriate security measures to secure their systems from cyber threats. The partnership will also

see the execution of joint projects aimed at supporting and accelerating the development of Indian start-ups in cyber domain, through Kaspersky Innovative Arm- Kaspersky iHub.

Public Wi-Fi Access Network Interface gets green signal

The Union Cabinet chaired by the Prime Minister, Shri Narendra Modi has given its approval for setting up of Public Wi-Fi Networks through the Prime Minister Public Wi-Fi Access Network Interface (PM-WANI**)** scheme.

PM-WANI eco-system will be operated by different players- Public Data Office (PDO), Public Data Office Aggregator (PDOA) and App Providers. Pricing of such services would be determined by market forces.[4]

According to the National Digital Communications Policy 2018,[5] India's digital profile and footprint is one of the fastest growing in the world with the highest mobile data consumption in the world and half a billion internet users. The last few years have also seen a rapid expansion of digital payments. It is estimated that India's digital economy has the potential to reach one trillion USD by 2025.

PM-WANI will help proliferation of public Wi-Fi that in turn will help achieve the goals of creating a vibrant and digital India. It will also help create employment in the country and help small and medium entrepreneurs in doing business and in turn boost the GDP of the country.

Due to the covid-19 pandemic, there has been a demand for more digitized work, e-commerce, and people to people connectivity. Deployment of Public Wi-Fi can help achieve these goals by delivery of stable and high speed Broadband Internet (data) services to citizens in areas which do not have 4G mobile coverage. Also, under the National Digital Communications Policy 2018, the pan-India count of WiFi hotspots target is of 5 million by 2020 and 10 million by 2022. PM-WANI is a focused step in the direction of creation of a Digital India.

The SolarWinds cyberattack

The attack on Solarwinds was discovered by US cyber security company, FireEye that provides security to many government and private companies. SolarWinds has almost 300,000 customers across the globe including government and private agencies. FireEye stated that as many as 18000 companies and agencies were impacted by the attack.[6] According to a New York Times report, parts of the Pentagon, Centres for Disease Control and Prevention, the Justice Department, and many others were victims of the attack.[7] The US nuclear weapons agency and at least three states were also hacked.[8]

The cyberattack is being marked as a supply-chain attack, in which trojanized versions of Solarwinds' Orion software was made available as a software update. The 18000 customers who were impacted, had updated their systems using the infected Orion software. The Orion update contained a malware called 'sunburst', which was capable of accessing system files/information of client systems which in turn, gave hackers a backdoor entry.

Even Microsoft, the largest software maker has found traces of the malware in their systems.[9] Microsoft is one of the largest providers of cloud services to a substantial population of the world, so an attack on its servers could impact a larger number of customers further. Also several other big tech companies, Cisco, Intel, Nvidia, Belkin, and VMware have all had computers on their networks infected with the malware.[10] The full extent of the hack and data theft is still being investigated.

FireEye CEO, Kevin Mandia called the hackers as "highly trained in operational security" as they relied on "multiple techniques" to avoid being detected. Several US government officials have also pointed fingers at Russia though there has not been any evidence of this.[11]

Global outage of Google

On 14th December, 2020, a global outage of Google services occurred for approximately 47 minutes.[12] This disrupted core services like Gmail, Google Drive, Google Docs, Google Meet, Google voice. Soon after, Google released a report mentioning the cause of the outage as an issue in its authentication platform. A second outage also occurred the next day, in which the Gmail service was down for two hours. An abrupt disruption of Google services had also occurred earlier this year in November.

Users across the world were unable to access Google services during the outage. Approximately 15% of requests to Google Cloud Storage (GCS) were impacted during the outage, specifically those using OAuth, HMAC or email authentication.[13]

The reason for the outage is reported to be unintended quota (of various resources allocated for services) changes due to an ongoing migration of the User ID Service to a new quota system. Despite having safeguards in place to prevent such crashes, the company's internal tools failed to allocate enough storage space to the services that handle authentication.

The widespread disruption of Google services for just half an hour has shown how severely our digital dependence has grown. Tech Giants like Google create a massive impact in our daily to day lives. Google smart home services and Google Assistant caused real problems when people around the world were unable to even turn on the lights of their homes using voice command.[14] Many other applications that are linked to Google, for example, Nest thermostats, were unable to control the heating mechanism of buildings. This certainly demands an increased spending on the reliability and testing of such services to prevent such incidents in the future.

[1] Grant Award View - GA137184 at https://www.grants.gov.au/Ga/Show/9d5fc489-7412-4aa7-a997-03a6a572f76a

[2] Australia spends $500,000 to strengthen tech ties with Quad allies amid China tension at https://www.theguardian.com/australia-news/2020/nov/23/australia-spends-500000-to-strengthen-tech-ties-with-quad-allies-amid-china-tension

[3] Kaspersky joins hands with CERT-In to keep cyber threats at bay, focus on privacy protection at https://economictimes.indiatimes.com/magazines/panache/kaspersky-joins-hands-with-cert-in-to-keep-cyber-threats-at-bay-focus-on-privacy-protection/articleshow/79529391.cms?from=mdr

[4] Cabinet approves setting up of Public Wi-Fi Networks at https://pib.gov.in/PressReleasePage.aspx?PRID=1679342#:~:text=This%20Public%20Wi%2DFi%20Access,deliver%20broadband%20services%20to%20subscribers.

[5] National Digital Communications policy 2018 at https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf

[6] https://indianexpress.com/article/technology/tech-news-technology/fireeye-stumbled-across-solarwinds-breach-while-probing-own-hack-7105407/

[7] FireEye stumbled across SolarWinds breach while probing own hack at https://indianexpress.com/article/explained/us-solarwinds-hack-cybersecurity-fireeye-russia-7110550/

[8] U.S. Nuclear Weapons Agency Hacked as Part of Massive Cyber-Attack at https://time.com/5922897/us-nuclear-weapons-energy-hacked/

[9] Microsoft says its systems were exposed to SolarWinds hack at https://indianexpress.com/article/technology/tech-news-technology/microsoft-says-its-systems-were-exposed-to-solarwinds-hack-7109396/

[10] Big tech companies including Intel, Nvidia, and Cisco were all infected during the SolarWinds hack at https://www.theverge.com/2020/12/21/22194183/intel-nvidia-cisco-government-infected-solarwinds-hack

[11] Explained: A massive cyberattack in the US, using a novel set of tools at https://indianexpress.com/article/explained/us-solarwinds-hack-cybersecurity-fireeye-russia-7110550/

[12] Google services including Gmail hit by serious disruption at https://news.sky.com/story/google-services-including-gmail-hit-by-serious-disruption-12052892

[13] Google Cloud Infrastructure Components Incident #20013 at https://status.cloud.google.com/incident/zall/20013

[14] Google suffers global outage with Gmail, YouTube and majority of services affected at https://www.theguardian.com/technology/2020/dec/14/google-suffers-worldwide-outage-with-gmail-youtube-and-other-services-down