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

CYBER *Digest*

July 2021

- **Major global internet outage takes websites offline**
- **Facebook to ban Trump for the next two years**
- **Cybercrime takedowns in June**
- **Helpline '155260' to Prevent Cyber Fraud**
- **PM warns about internet 'vulnerabilities' at G7 summit**
- **UNGGE on Cybersecurity adopts consensus report**
- **India in recent global cybersecurity rankings**

Major global internet outage takes websites offline

A major global internet outage was experienced on June 8 in which online businesses like Reddit, Amazon, Spotify and many other e-commerce websites went offline for almost an hour. Websites of the Guardian, the BBC, the New York Times and CNN were impacted. Some national government websites like gov.uk and the White House website also got affected, thus making the outage a broad and a severe one.[1]

The affected websites used the content delivery network (CDN) called Fastly which provides greater reliability and performance for heavily trafficked websites and handles 10% of the world's internet traffic. Fastly detected the disruption, caused by an undiscovered software bug that was triggered by a valid customer configuration change, and disabled the configuration. It took around 49 minutes for the network to get back to normal operations.[2]

A CDN is a global network of servers that provide content faster and protects websites from traffic overload. CDN failures are not new; in 2020, two other major failures were that of Cloudflare in July and Google in March. However, increased reliance on the internet in the pandemic era has meant that their impact has been felt much more. These outages also highlight the dangers of dependence on a few major internet services providers and the tendency towards centralisation of these services.

Facebook to ban Trump for the next two years

Facebook announced on June 4 that former president of the US, Donald Trump will remain suspended for two years from Facebook after he shared posts praising the violent US Capitol insurrection.[3] Facebook announced that the actions of the former President constituted a severe violation of their rules which merit the highest penalty available under the new enforcement protocols.

The Oversight Board upheld the suspension and stated that the decision was necessary.[4] The board also stated that the unprecedented circumstances justified the exceptional measures that were taken. It made a number of recommendations on improvement of policies which though are not binding, but would be actively sought and carefully reviewed by Facebook. Facebook has also stated that when the ban expires in 2023, the company will re-assess whether the risks to public safety have receded before lifting the ban.

Trump has called the ban as an "insult" and a means of censoring and silencing him.

Cybercrime takedowns in June

There were major successes recorded by law enforcement agencies in the fight against cybercrime in June. This was on the back of better international co-operation and co-ordination and these efforts show that the menace can be tackled once the coordination mechanisms are in place.

a) Asian cybercrime takedown leads to intercept of $83 million

Southeast Asian law enforcement agencies in a first of its kind operation called Operation Haechi-I, intercepted $83 million over the course of six months from September 2020 to March 2021.[5]

Operation Haechi-I is planned to continue over the next three years and is aimed at tackling financial cybercrime, combating investment fraud, money laundering linked to illegal online gambling and phishing. The

key factors in intercepting illicit money transfers, according to agencies, are speed and international cooperation- faster reporting of crimes by victims to the law enforcement agencies allow their funds to be recovered faster and cyber criminals being punished.

b) Slilpp marketplace shutdown

The Tor-based market on the Dark Web called 'Slilpp' has been shut down as per an announcement made by the U.S. Department of Justice (DOJ). Slilpp was responsible for dealing in stolen credentials on the dark web. It offered its users access to as many as 1,400 websites, 80 million accounts and services worldwide on the dark web market.[6]

A coordinated approach, international cooperation of FBI with a number of law enforcement agencies in Europe was required to perform this operation which eventually helped to eliminate various servers and domains used for the illicit market.

c) Hundreds arrested in global cybercrime bust

In a joint operation by Australia and the FBI, more than 800 suspected cyber criminals have been arrested worldwide after being tricked into using an FBI-run encrypted messaging app called ANOM. Devices with the ANOM app were secretly distributed among criminals that allowed the police to monitor their chats about drug smuggling, money laundering and other crimes.[7]

The operation which was conducted across a dozen countries, led to recovery of drugs, weapons, luxury vehicles and cash- eight tonnes of cocaine, 250 guns, currencies and cryptocurrencies worth more than $48million. The incident has been called a watershed moment by officials and has struck a heavy blow against organised crime around the world.

Helpline '155260' to Prevent Cyber Fraud

The Ministry of Home Affairs (MHA) has operationalised the helpline number 155260 as a reporting platform for financial losses due to cyber fraud.[8] Initially launched in Delhi in April 2021, the facility has now been extended to seven states and Union territories (Chhattisgarh, Delhi, Madhya Pradesh, Rajasthan, Telangana, Uttarakhand and Uttar Pradesh) and is expected to roll-out pan-India soon.

The move aims to provide a safe and secure digital payments eco-system especially due to the rising number of cyber fraud cases in the country. The platform would provide a mechanism for citizens who become a victim of cyber fraud, to report such cases and prevent the loss of their hard earned money.

The helpline been made operational by the Indian Cyber Crime Coordination Centre (I4C) in cooperation with the Reserve Bank of India (RBI). Most of the major banks, payment banks, wallets and online merchants are a part of the platform. The Citizen Financial Cyber Fraud Reporting and Management System has been developed in-house by I4C that would utilize new-age technologies for information sharing of online fraud cases and taking action in almost real time.

The facility empowers banks, the police, the law enforcement agencies and financial intermediaries to prevent the loss of defrauded money by following the money trail and stopping its further flow, before it is taken out of the digital system by cyber criminals. Since coming online, calls to the helpline have helped LEA stop the transfer of Rs.1.8 crores to fraudsters.[9]

PM warns about internet 'vulnerabilities' at G7 summit

As the G7 summit concluded at Cornwall, the leaders of the bloc, as well as guests invited to take part in the conclave reaffirming their shared belief in open societies, democratic values and multilateralism.
Indian Prime Minister, Shri Narendra Modi referred to India's civilizational commitment to democracy, freedom of thought and liberty. He highlighted the "revolutionary impact" of digital technologies on social inclusion and empowerment in India. He warned about "inherent vulnerabilities" in open societies and stressed "ensuring a safe cyber environment" on social media platforms.[10]

UNGGE on Cybersecurity adopts consensus report

The Report of the UNGGE on Advancing responsible State behaviour in cyberspace in the context of international security was adopted by consensus and will be submitted to the 76th session of the United Nations General Assembly in September 2021.

The report reflects the outcome of discussions carried out by the Group of Governmental Experts pursuant to General Assembly resolution 73/266 on 'Advancing responsible State behaviour in cyberspace in the context of international security'.[11]
The Group acknowledged and reaffirmed that an open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security. Respect for sovereignty and human rights and fundamental freedoms, as well as sustainable and digital development remain central to these efforts.
While ICTs and an increasingly digitalized and connected world provide immense opportunities for societies across the globe, serious ICT threats still persist. Incidents involving the malicious use of ICTs by States and non-State actors, harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally, have become increasingly serious.

The Group reaffirmed with regard to the use of ICTs by States that voluntary, nonbinding norms of responsible State behaviour can reduce risks to international peace, security and stability. Norms and existing international law sit alongside each other.

International law is the basis for States' shared commitment to preventing conflict and maintaining international peace and security and is key to enhancing confidence among States. The Group noted that by fostering trust, cooperation, transparency and predictability, **confidence-building measures (CBMs)** can promote stability and help to reduce the risk of misunderstanding, escalation and conflict. The support of the United Nations, regional and sub-regional bodies and other stakeholders can contribute to the effective operationalization and reinforcement of CBMs. **Exercising transparency** on a voluntary basis through the exchange of national views and practices on ICT security incidents and other related threats and by making ICT security advice, guidance, evidence base and data supporting decisions publicly available is important for building trust and predictability and helping organizations and agencies make good risk management decisions. The Group underscored the importance of **International cooperation and assistance in ICT security and capacity-building.** Increased cooperation alongside more effective assistance and capacity-building in the area of ICT security involving the private sector, academia, civil society and the technical community can help States apply the framework for the responsible behaviour of States in their use of ICTs.

Conclusions and Recommendations for Future Work: As States become increasingly dependent on ICTs, adhering to a common framework of responsible State behaviour in the use of ICTs in the context of international security is essential for all States to benefit from the technologies and protect against and respond to their misuse. The Group identified and provided greater clarity and guidance on the approaches States can take to ensure that cooperative measures effectively address existing and potential threats in the sphere of ICT security.

India in recent global cyber rankings

India ranks 10th in 2020 ITU Cybersecurity Index

The 4th iteration of the ITU Global Cybersecurity Index saw India climbing 37 places to No.10. Whilst the 2018 Index ranked India at 24, the 2019 Index had seen a precipitous fall in India's ranking to 47.[12]

The Index measured the engagement of member countries along four dimensions; legal measures, technical measures, organisational measures, capacity development and cooperation measures to arrive at its assessment.

IISS Cyber Net Assessment Report places India among Tier 3 nations

A report brought out by the International Institute of Strategic Studies (IISS) on "Cyber Capabilities and National Power: A Net Assessment" put India in Tier 3 clubbed along with Indonesia, Malaysia and Vietnam as a country in the early stages of its cyberpower development with strengths in some of the indicators on which it was assessed as well as significant weaknesses in other sectors.[13]

The report measured cyber power across seven indicators viz; strategy and doctrine; governance, command and control; core cyber-intelligence capability; cyber empowerment and dependence; cyber security and resilience; global leadership in cyberspace affairs and offensive cyber capability.

Whilst the assessments of these indexes are quite subjective as brought out by the widely differing rankings of India in these two reports, they nevertheless are useful in highlighting those sectors which need focussed intervention.

[1] Major internet outage 'shows infrastructure needs urgent fixing' at https://www.theguardian.com/technology/2021/jun/08/security-warning-error-cloud-websites-offline-outage

[2]Summary of June 8 outage at https://www.fastly.com/blog/summary-of-june-8-outage

[3] Facebook Will Ban Trump For The Next Two Years at https://www.buzzfeednews.com/article/janelytvynenko/facebook-will-ban-trump-for-two-years

[4]In Response to Oversight Board, Trump Suspended for Two Years; Will Only Be Reinstated if Conditions Permit at https://about.fb.com/news/2021/06/facebook-response-to-oversight-board-recommendations-trump/

[5] Asian cybercrime takedown leads to intercept of $83 million in financial theft at https://www.zdnet.com/article/asian-cybercrime-takedown-leads-to-intercept-of-83-million-in-financial-theft/

[6] Slilpp marketplace goes dark following government takedown at https://searchsecurity.techtarget.com/news/252502348/Slilpp-marketplace-goes-dark-following-government-takedown

[7] ANOM: Hundreds arrested in massive global crime sting using messaging app at https://www.bbc.com/news/world-57394831

[8] Government operationalises national Helpline 155260 to combat cybercrime losses, all you need to know at https://www.moneycontrol.com/news/india/government-operationalises-national-helpline-155260-to-combat-cybercrime-losses-all-you-need-to-know-7050761.html

[9] Govt launches national helpline no. to report cybercrime; all you need to know https://www.livemint.com/news/india/govt-launches-national-helpline-no-to-report-cyber-crime-all-you-need-to-know-11623950388095.html

[10] India makes G7 tone down criticism against internet shutdowns; PM warns about 'vulnerabilities' at https://www.deccanherald.com/national/india-makes-g7-tone-down-criticism-against-internet-shutdowns-pm-warns-about-vulnerabilities-997132.html

[11]Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security at https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/gge/documents/gge-report.pdf

[12] ITU Global Cybersecurity Index 2020 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[13] "Cyber Capabilities and National Power: A Net Assessment" https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power