Delhi Policy Group
Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

FEBRUARY 2022

Volume III, Issue 2 | February 2022

Delhi Policy Group
Core 5A, 1st Floor, India Habitat Centre, Lodhi Road, New Delhi- 110003
www.delhipolicygroup.org

Delhi Policy Group
Advancing India's Rise as a Leading Power

DPG Cyber Review
Vol. III, Issue 2
February 2022

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

DPG Cyber Review

This monthly publication is intended to cover major developments in cyber and digital technology domains and serve as a point of reference for national stakeholders committed to making cyber space a secure, trusted and vibrant tool for India's development and economic prosperity. It also aims to foster global cooperation to establish the rule of law in the cyber space. DPG Cyber Review is compiled by Brig. Abhimanyu Ghosh (Retd.), Senior Fellow for Cyber Security and Digital Technologies, from publicly available information and open source media. He can be reached at abhi.ghosh@dpg.org.in.

Cover Photograph:

World digital map

© 2022 by the Delhi Policy Group

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre,
Lodhi Road, New Delhi- 110003.
www.delhipolicygroup.org

DPG Cyber Review
Vol. III, Issue 2
February 2022

Contents

Abstract

India is one of the top five targets for cyber-attacks in the Asia Pacific region, primarily dominated by collusive attacks from Pakistan and China. The 'Long-Term Plan for China-Pakistan Economic Corridor (2017-2030)' that emphasises digital collaboration also extends to collusive cyber activities.

India banned 54 Chinese apps during the month, on grounds of national security, for illegally transferring data of its citizens to foreign servers. A total of 224 Chinese apps have so been banned, since the initial ban in June 2020.

Amid major concerns expressed by industry and privacy experts that it fails to sufficiently provide a data breach prevention and management framework, the Data Protection Bill 2021, finalised by the Joint Parliamentary Committee after extensive deliberations, is going to get a fresh look. The government is also planning to regulate data breach notifications by private players.

5G networks are likely to be rolled out by private players on August 15, so long as several pending issues pertaining to spectrum, technology and infrastructures can be streamlined. In the semiconductor space, India is looking to establish two greenfield fabs and two display fabs in the country.

The Russia-Ukraine war, which commenced on February 24, was preceded by cyber-attacks. Several websites of the Ukrainian government, army and major banks were affected by DDOS and data wiper attacks. But so far, these attacks have not been able to make any visible strategic impact on the conduct of the war.

Ukraine, which does not have a military cyber unit, has raised a voluntary "IT Army" to help protect critical infrastructure and conduct cyber espionage missions against Russian troops inside Ukraine. The "IT Army" supported by "Anonymous" activist groups have reportedly brought down or defaced several major Russian government and media websites. Several cybersecurity companies have also offered free tools and services to Ukraine. Starlink satellites of SpaceX have been activated to keep Ukraine online in case of terrestrial disruptions to its internet.

Cyberattacks have prompted Russia's National Coordination Centre for Computer Incidents to issue warnings to protect Russian critical information infrastructure and other information resources. Russia has also imposed restrictions on Facebook, YouTube and Twitter.

There has been a ransomware attack on the German oil and gas sector. Security agencies in the US and the UK have warned of cyber espionage operations by an advanced persistent threat (APT) actor, believed to be linked to the Iranian Ministry of Intelligence and Security (MOIS).

Chinese researchers working on 6G technology have claimed a new record for data streaming speed by sending 1 terabyte of data over 1 km (3,300 feet) in a second.

Indian companies are joining global consortiums for undersea cables, that serve as the strategic backbone for global internet connectivity.

National Developments

Pakistan-China collusion for cyber-attacks against India

On February 11, Russian cybersecurity firm Kaspersky released a report titled 'Cyberthreats to Financial Organisations in 2022' that identifies India as one of the top five targets for cyber-attacks in the Asia Pacific region, primarily dominated by collusive attacks from Pakistan and China. Most attacks are by the Advanced Persistent Threats (APT) that exploit gaps in cyber defences, and remain undetected for a long time. The 'Long-Term Plan for China-Pakistan Economic Corridor (2017-2030)', that emphasises digital collaboration, apparently extends to collusive cyber activities with the intention to collect valuable geopolitical, business, and military data. Most recently, Pakistan-based hackers conducted a major cyber-attack targeting India's power generation and transmission sector using a platform supplied by China Mobile Limited to Pakistan. Evidence of Pakistan's emergence as China's proxy have been found in misinformation-based influence operations, espionage and honey traps. During the ongoing border stand-off between India and China along the Line of Actual Control, Pakistan-based Twitter handles posing as Chinese nationals have peddled anti-India propaganda.

With China-Pakistan cyber collusion becoming a reality, India must prepare for the spectre of a 'two-front Cyber war'.[1]

Indian Army Personnel targeted by Fake Apps

The cyber threat intelligence firm Cyble reported on January 28 that threat actors replicated the legitimate apps used by military personnel and added malicious code into the fake app's source code. The apps identified are ARMAAN and HAMRAAZ, which were reportedly duplicated and embedded with malicious trojans. Upon successful execution, the fake app could steal sensitive data such as contacts, call logs, messages, location, files from external storage etc., from the victims' devices.

The Army Mobile Aadhaar App Network (ARMAAN) is an umbrella application covering various facets of information and services concerning all ranks of the Indian Army, while HAMRAAZ is an android application that provides access to salary-related information, and grievance management services. It was reported on February 7 that these fake apps have been removed from Play Store.[2]

[1] Pakistan collaborating with China in cyber attacks against India (imrmedia.in)
[2] Cyble — Indian Army Personnel Face Remote Access Trojan Attacks

India issues order to ban another 54 Chinese apps

On February 14, the government banned 54 Chinese apps, terming them a threat to national security. A number of these apps, owned by Alibaba, Tencent or NetEase, are "rebranded or rechristened avatars" of banned apps that have either changed ownership or are hosted out of Singapore or Hong Kong. A number of these apps are messaging, gaming and dating apps. A total of 224 Chinese apps have so far been banned since June 2020, following violence at the LAC in Ladakh.[3]

The ban was implemented under Section 69(a) of the Information Technology Act, 2000 on the grounds of illegal transfer of sensitive data of Indians to servers in China that are shared with its intelligence agencies. On February 18, China expressed concern over India's recent ban, and hoped that the same be reviewed in the interest of bilateral economic and trade cooperation.

Ransomware hits Jawaharlal Nehru Port Container Terminal

It was reported on February 22 that a suspected ransomware attack had knocked-out the management information system (MIS) at Jawaharlal Nehru Port Container Terminal (JNPCT), located in India's top container gateway of JNPT (Nhava Sheva). The attack was detected on February 21 and the port authority has been working to restore the critical operating systems. The other private terminals at JNPT are operating normally. The attack happened even as cyber security has become a top operational priority for container supply chain stakeholders since the crippling "Petya" cyber-attack on Maersk in June 2017.[4]

Data Protection Bill 2021 likely to be reworked

India is ranked third globally in terms of the number of data breaches, with an estimated total of 86.63 million breaches until November 2021.[5] The absence of a comprehensive Data Privacy Law is affecting India's digital innovations and e-commerce and this remains a major concern.

The Joint Parliamentary Committee (JPC) that reviewed the 2019 Personal Data Protection Bill (PDPB), came up with a new Data Protection Bill, 2021, with provisions to regulate non-personal data. The Bill was to be tabled in the next session of Parliament beginning on March 14. However, amid concerns of industry and experts that it fails to sufficiently provide a data breach prevention

[3] chinese apps: Govt issues order to ban 54 Chinese apps, Telecom News, ET Telecom (indiatimes.com)

[4] https://theloadstar.com/ransomware-attack-hits-nhava-sheva-container-terminal/

[5] Indian Data Privacy Regime: Stuck In An Endless Loop? - Privacy - India (mondaq.com)

and management framework, the 2021 Bill is likely to get a fresh look. Some of the contentious clauses include having a single regulator for non-personal and personal data, treating social media as publishers, localisation norms and making state security its core concern, at the cost of citizen's privacy rights. The major area of concern is the broad exemptions given to security agencies, without due scrutiny, under Section 35 of the Bill.

The information technology sector had petitioned the government that the Bill in its present form will adversely impact the fortunes of India's $190 billion IT-BPM industry in the European Union. Further, in a filing with the US Securities and Exchange Commission (SEC), Meta (formerly Facebook) and Google had expressed concern over regulatory hurdles proposed in the Bill. The fresh draft is expected to address all concerns and be compatible with the ongoing changes in local and global technologies to fuel growth of India's robust start-up ecosystem.[6] India's ambition of becoming $5 trillion digital economy depends on its ability to harness the value of data by effective regulation.

New regulation for organisations to report data security breaches

In addition to the above legislation pertaining to data privacy and security, the government is planning to regulate data breach notification. Data breach notification and incident response are currently loosely governed under the Information Technology Act, 2000 (ITA) and the ITA rules. It was reported on February 24 that the government is working on comprehensive laws that will prevent corporations from hiding security and data breaches. This will enable the government and its agencies to have clear situational awareness of the threat matrix that is active in cyberspace in India.[7]

On February 21, the government shared the new draft policy framework 'India Data Accessibility and Use' for public consultation. The framework will give measured access to suitably "anonymised" data to governments, start-ups, researchers and enterprises. The framework entails 'India Data Office', India Data Council, and Data Management Units as key components. The new policy will create a robust data sharing eco-system and enable better delivery of citizen centric services, through novel monetisation models, to aid Ministries and Departments in identifying and sharing priced data sets. Legal and privacy experts have raised concerns about "privacy" and "monetisation" of citizen data, as the current Information Technology Act, 2000 has no provision to govern

[6] Fresh legislation may replace Data Protection Bill - The Economic Times (indiatimes.com)

[7] New regulations to put onus on organisations to report data security breaches, IT Security News, ET CISO (indiatimes.com)

personal data usage by the government. Public feedback has been sought by March 18.[8]

Efforts towards a holistic cybersecurity policy

National Cyber Security Strategy has been in the making since 2020, and is pending approval. Efforts are on to give a fresh look to draft a comprehensive National Cyber Security policy. It was reported on February 12 that the National Security Council Secretariat has held a meeting with stakeholders to discuss expanding the ambit of cybersecurity policy to include sectors of health and water. The focus will be on identifying critical infrastructures, followed by an assessment of threats and vulnerabilities, both internal and external, and finally an action plan to counter these. In the process, NSCS will evaluate policies rolled out by the United Kingdom and Australia. The issue was reportedly also discussed on February 11, at the sidelines of the Quad ministerial held in Melbourne.[9]

On February 25, the Indian PM asserted that issues regarding cyber security were not limited to the digital world, but are a matter of national security.[10]

5G Launch in India likely on August 15

The rollout of 5G networks by private telecom operators in 2022-2023 was announced during the presentation of the Union Budget on February 1. However, the launch is dependent on several key issues, the primary one being the auction and allocation of 5G spectrum of frequencies. On February 8, the Telecom Regulatory Authority of India (TRAI) has embarked on the last phase of industrywide deliberation to finalise its views on pricing and optimisation of available radio waves. It was reported on February 22 that the Prime Minister's Office (PMO) has requested the Department of Telecom (DoT) to work towards the initial launch of 5G by 15th August, 2022, and also explore the possibility of obtaining requisite recommendations from TRAI before March this year.[11]

Besides the spectrum costs, the recommendations would include norms for new frequencies in various frequency bands. The allocation of mmWave (28 GHZ) has remained a contentious issue between terrestrial network operators

[8] Experts flag lack of laws on govt use of citizen data, IT Security News, ET CISO (indiatimes.com)

[9] India looks to redraw plan for cybersecurity policy: Officials | Latest News India - Hindustan Times (ampproject.org)

[10] Cyber security is a matter of national security: PM Modi, Government News, ET Government (indiatimes.com)

[11] 5g auction: DoT asks Trai to speed up 5G pricing views, says PMO wants initial launch by Aug 15, Telecom News, ET Telecom (indiatimes.com)

and satellite service providers on grounds of interference and auction/administrative allocation of Satellite frequencies. Both Reliance Jio and Airtel have applied for a 'global mobile personal communication by satellite services' (GMPCS) licences. Another issue pertains to the spectrum in the 'E' band (71-76 GHZ and 81-86 GHZ), which is ideal for strong mobile broadband backhaul network. Issues pertaining to sub-GHZ and mid-band frequencies have been raised. All stakeholders have been asked to file their inputs by February 15.[12]

All telecom players are also conducting 5G trials with new use cases, network slicing platforms and Open Radio Access Network (O-RAN), with their own equipment and enterprise partners. Use cases include trials of robotics, AI multimedia chatbot, and immersive high-definition virtual reality (HD VR) meetings. In the standards space, merger of the indigenous 5G Radio Interface Technology (5Gi) with the global 3GPP standards is awaiting formal approval of the International Telecommunication Union (ITU). Following the approval, the chip makers, telecom equipment manufacturers, handset producers, and other infrastructure providers would need to conform to new standards.

Indian private telecom and device makers have also joined the global O-RAN alliance, working on contributing to standards for open and multi-vendor RAN networks. The members of this global industry alliance include Airtel, Reliance Jio, state-owned Centre for Development of Telematics (C-DoT), HFCL as well as global companies including Nokia, Ericsson and Cisco.[13]

Concerted efforts towards Semiconductor Chip manufacturing

India consumed ₹1.1 lakh crore ($ 14.5 Billion) worth of semiconductor chips in 2020. On February 11, in a written reply to the Parliament, it was acknowledged that this domestic demand was currently met through imports, in the absence of commercial semiconductor fabs in India.

To correct the anomaly, a $10 Billion commercial semiconductor manufacturing programme was announced last December. On February 14, Vedanta group and Hon Hai Technology Group (Foxconn), which has a global footprint in electronics manufacturing, announced partnership for a $8 billion chip manufacturing plant for the manufacture of 28 nanometre chips that would be ready by 2024.[14] Further, Vedanta's group firm Avanstrate is expected

[12] vodafone idea: Telecom carriers, space broadband providers spar on mmWave band, seek interference resolution, Telecom News, ET Telecom (indiatimes.com)

[13] hfcl: HFCL joins O-RAN Alliance to drive 5G gear development, Telecom News, ET Telecom (indiatimes.com)

[14] https://swarajyamag.com/tech/vedanta-and-foxconn-sign-pact-for-manufacturing-semiconductors-in-india

to roll out electronic chips and displays from Indian manufacturing plants by 2025, with an investment of up to $20 bn in semiconductor businesses. Another proposal has been received from Abu-Dhabi based Next Orbit Ventures for a 65-nanometre fab at the cost of $3 billion in collaboration with Israeli Tower Semiconductor as its technology partner. But the number of applicants, as on the last date-February 15, remains small. The complete evaluation and signing of agreements with companies is expected in 8-10 months.[15]

The government is cognisant of the fact that companies may need more time to submit formal applications given the scale of the commitment of $3-5 Billion for a typical semiconductor chip-making plant. India is looking to approve proposals for establishment of at least two greenfield semiconductor fabs and two display fabs in the country. Positive movement is expected after recent high-level discussions with the world's five largest chip manufacturers.

IISc commissions Param Pravega supercomputers in India

On Feb 04, 2022, the Indian Institute of Science (IISc) installed and commissioned Param Pravega, one of the most powerful supercomputers in India, under the National Supercomputing Mission (NSM). The system, which is expected to power diverse research and educational pursuits, has a total supercomputing capacity of 3.3 petaflops (1 petaflop equals a quadrillion or 10^{15} operations per second). It has been designed by the Centre for Development of Advanced Computing (C-DAC). A majority of the components used to build this system have been manufactured and assembled within the country, along with an indigenous software stack developed by C-DAC, in line with the "Make in India" initiative.[16] The NSM is steered jointly by the department of science and technology (DST) and the ministry of electronics and information technology (MeitY). It has so far deployed 10 supercomputer systems with a cumulative computing power of 17 petaflops.

[15] semicondudctor manufacturing: Government to extend window for applications to chip scheme, Telecom News, ET Telecom (indiatimes.com)

[16] https://m.economictimes.com/tech/technology/iisc-commissions-param-pravega-one-of-the-most-powerful-supercomputers-in-india/amp_articleshow/89315303.cms

International Developments

Russia-Ukraine War and the game in Cyberspace

The Russia-Ukraine war, which commenced on February 24, was as expected preceded by cyber-attacks, mostly on Ukrainian territory. The Russian strategy of wedding cyber operations with physical aggression has historical precedence. But so far, these attacks have remained below par and have not been able to make any strategic impact on the conduct of the war.

On February 15, a series of cyberattacks knocked out the websites of the Ukrainian army, the defence ministry and major banks, as tensions persisted over the threat of a possible Russian invasion. A month ago, on January 14, another strike briefly took down key government websites. Kyiv said the damage in January had been limited. The Kremlin had denied responsibility.

As the conflict commenced, the websites of Ukraine's defence, foreign and interior ministries were unreachable or painfully slow, after a series of distributed-denial-of-service attacks in concert with kinetic attacks on Kyiv and other major cities of Ukraine. In addition to DDoS attacks, Ukraine computers were hit by data-wiping software. ESET Research Labs reportedly detected the malware that impacted roughly 50 computers, mostly in financial outfits. Symantec Threat Intelligence detected three organisations hit by the wiper malware — Ukrainian government contractors in Latvia and Lithuania, both members of NATO, and a financial institution in Ukraine.[17] NATO responded within hours of the attacks by announcing a cyber warfare cooperation deal with Kyiv. NATO Secretary General Jens Stoltenberg warned that cyberattacks could trigger NATO's Article 5, which considers an attack on any NATO ally an attack on all.[18]

To waive off the barrage of cyber-attacks, the Ukrainian government, on February 24, asked for volunteers from the country's hacker underground to help protect critical infrastructure and conduct cyber espionage missions against Russian troops inside Ukraine. Volunteers have been asked to submit applications via Google docs, listing their specialties, such as malware development, and professional references.[19] On February 26, Ukrainian Minister of Digital Transformation Mykhailo Fedorov called for volunteer hackers to follow a Telegram channel dedicated to listing potential targets,

[17] Cyberattacks accompany Russian military assault on Ukraine | AP News
[18] https://www.securityweek.com/russia-vs-ukraine-war-cyberspace
[19] Ukraine calls on hacker underground for defence against Russia - BusinessToday

saying on Twitter, "There will be tasks for everyone. We continue to fight on the cyber front."[20]

Ukraine does not have a dedicated military cyber force. Therefore, the effort to build an "IT Army" has come late but has started showing results. Several major Russian government and media websites have been intermittently offline, with many attributing the outages to DDoS attacks. Websites for the Russian Foreign Ministry as well as the country's largest stock exchange and a key state-owned bank were offline on February 28. Simultaneously, members of the "Anonymous" hactivist movement have reportedly defaced Russian websites and leaked data allegedly stolen from high-profile organisations, including the Russian Ministry of Defence. "Anonymous" hackers have also claimed responsibility for disrupting the websites of pro-Kremlin Russian media, and defaced them with antiwar messaging.

These attacks have prompted Russia's National Coordination Centre for Computer Incidents to issue warnings to protect Russian critical information infrastructure and other information resources. Some criminal ransomware operators have pledged loyalty to the Kremlin, suggesting contested game at the digital front of the deadly conflict.

Social media networks have also become one of the fronts in the Russia-Ukraine war. These platforms have become home to misleading information and real-time monitoring of a quickly developing conflict that marks Europe's biggest geopolitical crisis in decades. On February 25, Facebook restricted Russian state media's ability to earn money by running ads or monetising anywhere in the world on the social media platform, as Moscow's invasion of neighbouring Ukraine reached the streets of Kyiv.

The war in the information space has prompted the Russian government to issue an alert to the media regarding the circulation of false information. The country's Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) has warned YouTube after they suspended the accounts of several Russian media organisations. It also imposed restrictions on Facebook and Twitter, after they refused orders to stop using fact-checkers and content warning labels on its platforms.

On February 28, the Ukrainian President signed an official request for Ukraine to join the European Union. EU has promised to mobilise "all its resources"

[20] Volunteer Hackers Join Ukraine's Fight Against Russia - WSJ (ampproject.org)

including in cyberspace to help Ukraine. The full tempo of the war in Cyberspace is yet to unfold.

Starlink satellites activated to give Ukraine data backup

SpaceX has thousands of Starlink satellites in orbit, which beam broadband services around the Earth without the need for fibre-optic cables. On February 27, SpaceX founder Elon Musk activated Starlink in Ukraine, and despatched several ground terminals. The satellites could keep Ukraine online if its internet infrastructure is damaged by Russia's attacks. Activation came in response to a plea by Ukraine's First Vice Prime Minister and Minister of Digital Transformation, who called for help on February 26, as Ukraine fought off kinetic invasion and sustained cyberattacks by Russian forces.[21]

Another US listed Satellite company Viasat Inc said on February 28 that it was investigating a suspected cyberattack that caused a partial outage in its residential broadband services in Ukraine and other European countries. The outage could have been due to a distributed denial of service (DDOS) attacks that had hit a number of Ukrainian banks and government websites shortly before Russia's invasion.[22]

Russia could use crypto currencies to blunt US sanctions

On February 24, the US President imposed "devastating sanctions" on Russia, blocking its banking sector and targeting Russian elites.

Russian entities are preparing to blunt some of the sanctions by making deals with anyone using digital currencies to bypass the control points that governments rely on — mainly transfers through banks using the SWIFT system. While sanctions imposed on Russia in 2014 were effective, the financial scenario has changed significantly since then. The global market for cryptocurrencies and other digital assets has grown, challenging the position of the dollar as the world's reserve currency and payments worldwide. Banks have to abide by "know your customer" rules, to verify their clients' identities, but Cryptocurrency exchanges rarely follow rules.

A new "digital rouble" would allow Russian entities to conduct transactions outside the international banking system with any country willing to trade in digital currency. China, Russia's largest trading partner in terms of both

[21] Elon Musk activates Starlink satellites to give Ukraine data backup – POLITICO

[22] viasat: Satellite firm Viasat probes suspected cyberattack in Ukraine and elsewhere, IT Security News, ET CISO (indiatimes.com)

imports and exports, has already launched its own central bank digital currency.

Meanwhile, the US is tightening monitoring of cryptocurrency activity. On Feb. 17, the Justice Department announced that it had created a new national cryptocurrency enforcement team to monitor cryptocurrency users. [23]

Major Twitter accounts reporting on Ukraine blocked

On February 24, some Twitter accounts that report on the situation in Ukraine with videos and photos showing Russian military operations on the ground were reportedly frozen. These are mostly Open-Source Intelligence (OSINT) platforms run by private-sector volunteers and other organizations that collect satellite imagery and other data. It is gathered that Russia had been reporting such tweets to Twitter with the aim of having these accounts frozen. Many of the locked accounts were not only analysing the movements of the Russian military, but were also referring to military intelligence experts to offer information about the developing situation.[24]

Ransomware attacks on Oil and Gas sectors in Germany

On February 7, the German Office for Information Security (BSI) announced that the BlackCat ransomware group was behind a recent cyberattack on two German oil companies that affected hundreds of gas stations across northern Germany. Oiltanking Deutschland GmbH & Co. KG terminals are operating with limited capacity and have declared force majeure. Mabanaft Deutschland GmbH & Co. KG has also declared force majeure for the majority of its inland supply activities in Germany. Reports suggest that multiple oil transport and storage companies across Europe are also dealing with cyber-attacks.[25]

Ransomware Targeted 14 of 16 U.S. Critical Infrastructure Sectors in 2021

Over the past several years, ransomware has become the most prevalent threat to organisations in private and public sectors alike, including financial services, food and agriculture, government, healthcare, and other critical infrastructure industries. In the U.S., ransomware attacks in 2021 targeted 14 of the 16 critical infrastructure sectors, as defined by the US Department of Homeland Security.

[23] Russia Cryptocurrency: Russia could use cryptocurrency to blunt the force of US sanctions - The Economic Times (indiatimes.com)

[24] https://asia.nikkei.com/Politics/Ukraine-conflict/Major-Twitter-accounts-reporting-on-Ukraine-blocked

[25] https://www.bbc.com/news/technology-60250956

In a joint advisory on February 10, cybersecurity agencies of the US, UK, and Australia have warned victims against paying ransom. Throughout 2021, ransomware incidents grew in sophistication, increasing the impact on cloud services, managed service providers, the software supply chain and industrial processes.

The ransomware landscape continues to evolve, backed by a complex network of specialised threat actors and affiliates engaged in malware development, distribution, and negotiation, sometimes leading to difficulties in attributing attacks to a specific group. Not only is Ransomware-as-a-Service (RaaS) growing, but attackers also rely on independent services to negotiate with the victims to facilitate ransom payments. In some instances, victims were directed to a 24/7 help center to assist with the payment and data recovery.[26]

US, UK Warn of Iranian Cyberattacks on Government Networks

On February 25, Cyber Security Agencies in the US and the UK warned of cyberespionage operations that the Iranian state-sponsored threat actor 'Muddy Water' has been running against both public and private sector organisations worldwide. Active since 2017, it is an advanced persistent threat (APT) actor, believed to be linked to the Iranian Ministry of Intelligence and Security (MOIS). This adversary is facilitating the Iranian government with stolen data and access to compromised networks in multiple sectors – including government, defense, telecoms, and oil and natural gas in Asia, Africa, Europe, and North America. In January 2022, the U.S. Cyber Command (CYBERCOM) made public several files associated with the 'Muddy Water' operations, including backdoor sample.[27]

China races ahead in 6G technologies

China is poised to become the leader in 6G technologies, even as the US and Japan had announced last April a $4.5 billion cooperative effort to challenge China's quick advances in 6G. It was reported on February 9 that Chinese researchers working on 6G technology have set a new record for data streaming speed with a novel technology using vortex millimeter waves, a type of extremely high-frequency radio wave with rapidly changing spins. The researchers sent 1 terabyte of data over 1 km (3,300 feet) in a second. Previously,

[26] https://www.securityweek.com/ransomware-targeted-14-16-us-critical-infrastructure-sectors-2021

[27] https://www.securityweek.com/us-uk-warn-iranian-cyberattacks-government-commercial-networks

in 2020, a team from Japan's Nippon Telegraph and Telephone Company had attained a speed of 200 Gbps over a distance of 10 meters (33 feet).[28]

Researchers at the Tsinghua University's School of Aerospace Engineering had set up the experimental wireless communication in the Beijing Winter Olympics compound, that could stream more than 10,000 high-definition live video feeds simultaneously. They also claim to have demonstrated that a hypersonic weapon could communicate and locate targets using 6G technology. The Tsinghua University team is also developing a prototype quantum radar using similar technologies that can detect even stealth planes.

According to a poll conducted by Nikkei and Tokyo-based research firm 'Cyber Creative Institute' in September 2021, China possesses more than 40% of the world's 6G patent registrations, followed by the US with 35%, Japan (10%), Europe (9%), and South Korea (9%).[29]

Beijing intends to enhance its funding for 6G research and development, as well as participate in the development of international 6G standards. The newly claimed feat could help China take the lead in the global race for next-gen 6G wireless communication.

Indian companies invest in global undersea cable consortiums

Undersea cables serve as the strategic backbone for global digital connectivity. Approximately 430 undersea fiber optic cables carry 99% of intercontinental internet traffic, and those lifelines of global commerce are highly vulnerable to natural and deliberate disruptions.[30] Indian companies including Tata, Reliance and Airtel stakes in global consortiums.

On February 21, Reliance Jio announced collaboration with Ocean Connect Maldives for constructing a multi-terabit India-Asia Xpress (IAX) undersea cable system. The high capacity and high-speed IAX system will connect the Maldives directly with major internet hubs in India and Singapore. The IAX originates in Mumbai and connects directly to Singapore, with additional landings in India, Malaysia, and Thailand. This would facilitate Maldives with a low latency cable system and bring down internet cost.

[28] Race to 6G: Chinese researchers declare data streaming record with whirling radio waves | South China Morning Post (scmp.com)

[29] 100 Times Faster, China Claims New 'World Record' In Data Streaming Using Next-Gen Wireless Communication (ampproject.org)

[30] US needs to temper reliance on at-risk undersea internet cables, satellites can help: Aerospace | Aerospace Center for Space Policy and Strategy

Jio would also construct the India Europe-Xpress (IEX) system that connects Mumbai to Milan, landing in Savona, Italy, and includes additional landings in the Middle East, North Africa, and the Mediterranean. IAX is expected to be ready for service by the end-2023, while IEX will be ready for service in mid-2024. IEX and IAX together, with speed of 100 Gbps over 16000 kms, will be important developments in telecommunications infrastructure, linking India, Europe to Southeast Asia, and now the Maldives.[31]

On February 21, Airtel announced that it will join a South East Asia–Middle East–Western Europe 6 (SEA-ME-WE 6) cable system that will go live in 2025. It will invest 20% of the overall cost to scale up its high-speed global network capacity to serve India's fast-growing digital economy The 19,200 KM SEA-ME-WE-6 cable system with 100 TB capacity will connect Singapore and France, and will be amongst the largest undersea cable systems globally. Airtel has acquired one fiber pair on the main SEA-ME-WE-6 system and will co-build four fiber pairs that will land in Mumbai and Chennai.

Undersea cables carry the risk of sabotage during geo-political conflicts like the current Russia – Ukraine crisis. Therefore, redundancy to these cable systems for diversity and access should remain a priority.[32]

Russia-Ukraine war may impact the semiconductor industry globally

The semiconductor ecosystem, already plagued by shortages due to the Covid-19 pandemic and technology cold-war, may get further stressed by the Russia-Ukraine war, leading to shortage of chips, long lead times, escalated prices and impact on all business verticals.

Both Ukraine and Russia are major players in global semiconductor supply chains. They produce important gases and rare earth metals, which are used in the lithography for the manufacture of chips. Ukraine is an important source for semiconductor-grade neon gas, which is a highly purified gas for etching circuit designs into silicon wafers to create chips. Russia is a key source of palladium used in many memory and sensor chips. In fact, Russia accounts for 45 per cent of the global supply of Palladium. It also produces several other key raw materials for computer chips, including the rare–earth metal, scandium.

The imposition of sanctions on Russia by the EU and G7 countries will further affect the global supply chain. On February 25, Japan announced sanctions on Moscow targeting semiconductor exports. Taiwan Semiconductor Manufacturing Company (TSMC), the world's largest contract chipmaker, has

[31] Reliance Jio: Jio to land IAX undersea cable system in Maldives in collaboration with Ocean Connect Maldives, Telecom News, ET Telecom (indiatimes.com)

[32] Airtel: Airtel joins undersea cable consortium to scale up global network capacity, Telecom News, ET Telecom (indiatimes.com)

pledged full compliance with new US export controls on technology supplies to Russia. Although direct semiconductor exports from Taiwan to Russia are minuscule, chips and other electronic components manufactured by its companies are contained in a much broader array of finished products sold to Russia by branded companies. The trickle-down effect of the war could potentially impact chip capacity and consequently, spike chip prices.[33]

[33] Russia-Ukraine war to cripple semiconductor industry globally - BusinessToday

International Cooperation

4th Quad Foreign Ministers Meeting

The 4th Quad Foreign Ministers' Meeting was held in Melbourne on February 11. In a Joint Statement after the meet, the ministers welcomed progress on the practical cooperation on counter-terrorism, countering disinformation and cyber security and resolved to strengthen capacity building. They also welcomed ongoing work in key areas including cyber security, infrastructure, and critical and emerging technologies.

The Quad will coordinate with partners across the Indo-Pacific to address the growing threat of ransomware. To promote international peace and stability in cyberspace, the Quad would help to build the capacity of regional countries to implement the Voluntary Norms for Responsible State Behaviour in Cyberspace, endorsed by UN.

The Quad ministers also expressed their commitment to strengthen diplomatic efforts so that the vision for technologies, guided by the Quad Principles on Technology Design, Development, Governance, and Use, will be further shared by all like-minded nations. The Quad is also exploring a track 1.5 dialogue on these issues between their respective strategic thinkers.[34]

***

[34] Joint statement by the Foreign Ministers of Australia, India and Japan and the Secretary of State of the United States following the 4th Quad Foreign Ministers' Meeting (mea.gov.in)

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre, Lodhi Road
New Delhi - 110003
India

www.delhipolicygroup.org