CCAOI™

Representing the ecosystem of Internet -Bharat Model

CCAOI Newsletter March 2022

Highlights of March

Most of the updates this month a related to the ongoing Digital war between Russia and Ukraine, the Online Safety bill, the EU-US Transatlantic Data Privacy Framework, Digital Markets Act, cybersecurity discussions at the UN OEWG and the First session of UN Ad Hoc Committee, ICANN73 meeting, anti-trust measures against Big Tech, Amazon-Future battle, and more.

Ukraine crisis: The Cyber war is on!

We continue to witness cyberattacks, slew of sanctions – economic as well as technology related on Russia, calls for cutting off Russia from the Internet, information warfare with content regulation measures by governments and platforms and more, leading to this crisis being labelled as the "first cyber war in human history" or "most viral war".

Cyberattacks and the blame game

The spate of cyberattacks continue with each side accusing the other.

Ukraine claims Russian hackers continue to attack Ukrainian sites. Ukrtelecom, a major internet service provider suffered a cyberattack and the Ukrainian State Service for Special Communications and Information Protection (SSSCIP Ukraine). attributed the attack to Russia. Ukraine has alleged Russia of targeting European refugee charities supporting Ukrainian refugees. Ukraine's Computer Emergency Response Team (CERT-UA) has cautioned of cyberattacks through fake antivirus updates ESET Researchers warned against a data wiping software "CaddyWiper"hitting Ukrainian networks.

The US and UK have pledged to support cyber security assistance to Ukraine.

Meanwhile, the USA is on high alert for cyberattacks on critical infrastructure and businesses from Russia. The FBI has warned that scanning of US energy sector companies have intensified from Russian IPs since the Ukraine conflict. Google's Threat Analysis Group reported that Russian hackers had attempted to penetrate the networks of NATO and the militaries of some eastern European countries. US President Joe Biden warned business leaders in the US to beef up their security. However, Russia has dismissed these warnings stating that it did not engage in 'banditry'.

Russia has claimed increase cyberattacks on government, media and critical infrastructure attributing them to Ukrainian hacker or their supporters. There have been reported cyberattacks on Russian companies such as Miratorg Agribusiness Holding; Russian information services . The websites of several Russian arbitration courts were defaced. Kaspersky has reported that the number of cyberattacks on Russian businesses has quadrupled in Q1 2022 vs Q1 2021. Hacking group Anonymous claimed taking down German subsidiary of the Russian oil company Rosneft; the website of Rosatom State Nuclear Energy Corporation, the websites of Moscow.ru, the Analytical Center for the Government of the Russian Federation, the Ministry of Sport of the Russian Federation, and Russia's Federal Security Service (FSB). The hackers group 'The Black Rabbit World', affiliated with Anonymous, claimed hacking the Central Bank of Russia, and releasing the stolen data.

The most Viral war?

Both Russia and Ukraine have been waging a viral war, each blaming the other for spreading fake news.

This month Ukraine claimed to have destroyed five bot farms backed by Russia that were spreading 'panic' among Ukrainian citizens.

After EUs call to ban Sputnik and Russia for spreading misinformation (which Switzerland opted out from) most Tech platforms Meta, Twitter, Twitch, Google have complied. However, Tech platforms have been reported to have taken additional steps apart from the ban, raising concerns and questions over the neutrality of big tech, the power they yield and whether they should have the authority to take such decisions. Questions are also being raised how business entities can overstep and take decisions that impact public at large.

It was reported that Meta changed its hate speech policy related to Ukraine- Russia and Poland and allowed post on Facebook calling for violence against invading Russians or Putin's death. Meta's policy change triggered angry response from the Russian government stating that it was considering designating Meta as a terrorist organisation. This prompted Meta to change the policy and Meta officials rushed to clarify that "We are only going to apply this policy in Ukraine itself". The company added that users cannot post messages to kill Russia's President Putin on Facebook due to the Ukraine war and that the company clarified that it has temporary eased its hate speech policy only to allow posts by users in Ukraine to making threats to Russian military in the context of its invasion of the country.

In retaliation Russia blocked Instagram, opened criminal case against Meta. Meta in turn has asked the Russian court to dismiss proceedings.

Google has been asked to stop spreading threats against Russians on YouTube and Russia's telecoms watchdog Roskomnadzor has drawn up two cases against Google for not removing banned content.

Roskomnadzor sent a notice to Wikimedia requesting removal of 'false information concerning the special military operation in Ukraine'.

Russia has introduced new Fake news law with harsh penalties such as penalties up to 15 years in prison for spreading fake news, making it unlawful to deliberately spread false information related to the Armed Forces of the Russian Federation. This law has resulted in several global media companies such as Bloomberg, EFE and others from leaving Russia

Cutting Russia off from the internet- a bad idea?

The calls to cut off Russia from the internet persist. ICANN rejected Ukraine's request and a civil society coalition has written to the US President calling to safeguard internet connectivity in Russia. Another group of experts have drafted guiding principles proposing rather that disconnecting the Internet, other solutions such as blocking websites can be more effective.

Two major backbone operators Lumen Technologies and Cogent Communications have exited Russia. However content delivery networks Cloudflare and Akamai are still providing services.

Owing to the sanctions, Russia's RSPP Commission for Communications and IT, the country's largest entrepreneurship union has expressed concern that shortage of equipment may lead to Internet outage, however the Russian Ministry of Digital Development has refuted the concerns.

Sanctions and more sanctions

Sanctions by the US and its allies against Russian technology and information services, with an intent to cripple its economy continues, along with exodus of companies from Russia.

Ukraine has called on software giants to stop supporting their products in Russia. It has legalised the cryptocurrency industry allowing foreign and Ukrainian cryptocurrencies exchanges to operate legally with Ukraine. It is reported that Ukraine is using Clearview AI Facial recognition technology (FRT) to identify Russian corpses and is planning to move of sensitive data overseas.

There have been several **sanctions against Russian companies.** The UK has imposed sanctions against on Russian media groups (RT, Rossiya Segodnya group) and 12 Russian citizens. The US has imposed sanctions on Russian technology companies producing chipsets, hardware, microelectronics, navigational equipment, etc.

The FCC is US has added Russian Kaspersky Lab to its list of equipment services that pose a threat to national security. UK has issued advisory to organisations providing services to Ukraine to rethink on using Russian technology or services. In Italy the public authorities have been asked to replace antivirus software developed by Kaspersky Lab. Germany has issued a warning that anti-virus software developed by Kaspersky Lab poses a serious risk of a successful hacking attack.

Tech Companies suspending services in Russia continue. Qualcomm announced suspending sale of products to Russian companies. Apple has stopped the Apple Pay service for Mir card payment system in Russia which till now allowed Russians to keep using Apple Pay even after the sanctions.

Measures continue **to curb Russia's use of crypto currency for evading the economic sanction.** The surge in the use of crypto is raising concerns among global financial regulators that it could be used to evade Western sanctions on Russia. Crypto firms are being asked to comply with the sanctions against Russia (Japan, UK) The US Treasury Department has reiterated that sanctions against Russia extend to crypto currency. The US and EU have agreed to share financial intelligence on illegal use of digital assets.

In the US the Democrats have introduced a bill to curb Russian crypto use and in a step towards cryptocurrency regulations the US President has signed an executive order for on ensuring responsible development of digital assets with the national agencies being instructed to develop appropriate regulations. While Japan plans to revise its foreign exchange laws to plug the crypto loophole in the sanctions

Meanwhile **to bypass the sanctions, and for encouraging domestic industry in Russia**, an executive order has been signed to boost its IT industry with funds from the federal budget in annual aid to be allocated to support promising IT solutions. Russia has banned government offices from purchasing foreign software and stop using foreign OS by 2025. Russian developers have launched Rossgram a Russian version of Instagram and are planning to launch an alternative to Google Play.

Further, Russia has approved 'parallel imports' of top brands without the trademark owners' permission, after top brands left the country. Further, a Russian court has overturned a ruling of 2021, that had proposed to bar Samsung Electronics from importing and selling 61 models of smartphones in Russia over an intellectual property lawsuit.

Online Safety Bill introduced in the UK Parliament

The Online Safety Bill that is aimed at creating a safer online environment for users, especially children, was introduced in the UK Parliament. Once approved by the Parliament, the bill will become a law.

There have been several changes in the bill since it was first published in May 2021. Some of the changes include: adding into the scope all paid-for scam advertisements in social media and search engine ; obligation of all websites which publish or host pornography to include checks and age gating; new measures to address anonymous trolls and criminalising cyberflashing.

The bill proposes obligations on social media platforms, search engines, websites and apps for protecting children online, tackling illegal content, and limiting the spread of misinformation.

Companies will have to proactively remove illegal online content related to terrorism and child sexual exploitation and abuse; report any child sexual exploitation and abuse content on their platforms to the National Crime Agency; address issues related to 'legal, but harmful content' ; ensure that their terms of service related to content moderation are consistent, transparent, unambiguous and uniform; prevent publishing and hosting of fraudulent advertisements on their services; websites hosting or publishing pornographic content to prevent anyone below 18 years cannot access them; develop clear and easy process to report harmful content and challenge content takedowns.

Companies failing to comply with these obligations can be fined by Ofcom up to 10% of their annual global turnover. Any company that fails to comply with the obligations can be fined up to10% of their annual global turnover by Ofcom the regulator. The bill introduces criminal liability of senior executives and also forces the companies to improve their practices.

Ofcom has been provided the power to block non-compliant sites, demand companies to provide data and information on how algorithms are used in content display and moderation.
Concerns have been expressed that the Online Safety Bill risks free speech, is a huge missed opportunity as it has several "gaping holes" and there remains more to be done to reduce harmful content online.

EU- US agree on new Trans-Atlantic Data Privacy Framework

The EU and USA in principle agreed on a new Trans-Atlantic Data Privacy Framework, which will replace the earlier Privacy Shield which was invalidated after Shrems II ruling. While the joint statement mentioned the commitment to implement safeguards to ensure safety of the personal data of EU citizens, however no text of the framework was released.

The Privacy Shield, which allowed US companies to transfer data of European users to the USA in compliance with GDPR standards, was invalidated in 2020 by the Court of Justice of the EU (CJEU), and the ruling is better known as Schrems II ruling, after Max Schrems an Austrian activist who initiated the proceedings

Reacting to the announcement, Shrems stated that it is a political deal, will probably take month for any text to be drafted and more importantly, solutions would still need to be found to the concerns raised by the CJEU.

EU reaches provisional agreement on Digital Markets Act

This month the European Parliament and the Council reached a provisional political agreement on the Digital Markets Act (DMA) that is aimed to make the digital sector fairer and more competitive in the EU. The next steps would involve polishing the technical details and getting the final approval by the Parliament and the council to become a law.

The DMA defines rules for large online companies and aims to clamp down on antitrust behaviour of those that act as "gatekeeper". “Gatekeepers” have been defined as companies that have an annual turnover of at least €7.5 billion within the EU (or a market valuation of at least €75 billion), at least 45 million individual monthly users and 10,000+ business users in the EU. Further DMA establishes obligations for gatekeepers, such as, need to ensure certain levels of interoperability and access to marketing data, not being allowed to pre-install certain software or rank their products higher than their competitors.

Privacy concerns have been expressed by critics over the “interoperability” requirement especially in end-to-end encrypted messaging platforms. As the final text is yet to be released several suggestions are being proposed by the community on what aspects should be focused on to ensure security and privacy of EU citizens.

Issue based updates:

Cybersecurity

UN Ad Hoc Committee First session update

The first session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, was organised from 28 February to 11 March. While Russia had proposed these negotiations, during the session several member states expressed concerns over Russia's engagement in the negotiations in light of the Ukraine crisis. The main topic of this session was procedure, and the member states adopted the draft report and its addendums one through seven.

During a discussion on the proposed text of the Cybercrime Treaty divergent views were expressed by member states on several aspects such as, what differentiates cybercrime and cyber-dependent crime, if and how human rights protections will apply and be reflected in the treaty, balancing the implementation of the treaty through criminal justice and law enforcement mechanisms while upholding human rights, etc.

The Roadmap for the next steps of this negotiations was adopted by the committee. As next step member states were expected to provide specific drafts on the Preamble, General provisions, provisions on Criminalization, Procedural measures and Law Enforcement of the negotiating text before by 8 April which would be discussed in the second meeting (30 May–10 June 2022)

UN OEWG Second Substantive Session

The UN Open-Ended Working Group (OEWG) held its second substantive session between 28 March–1 April mostly in an informal mode. While the group started work from June 2021, there are disagreements on how stakeholders will participate in the working group. As a result, the provisional program was not adopted by the member states and the session could not be conducted in a formal mode. The substantive issues were then discussed in an informal mode. These include issues related to the existing and potential threats in the ICT sphere and data security; rules, norms, and principles of responsible behaviour of states in cyberspace; how international law applies to the use of ICTs by states; confidence-building measures; and capacity building.

In terms of **reported cyberattacks**, several Israeli government websites including the websites of the ministries of interior, defence, justice and Prime Minister’s Office were hit due to a DDoS attack against a communications provider. Hackers stole about $600 million from a blockchain network connected to the popular online gaming site Axie Infinity .Samsung faced a data breach where the hackers stole internal company data and source code for Galaxy devices. Hacking group Lapsus$ has claimed responsibility. In India, servers of Mahesh Cooperative Urban bank were compromised and hackers siphoned off over Rs 12 crores(INR).

Child Safety continues to be in the spotlight**.** The Cyberspace Administration of China has issued a new draft regulation for protecting children. Companies engaged in online gaming, livestreaming, audio and video in

China will have to set up a "youth mode", conduct regular assessments to protect minors online and even cap daily spending amount for minor users. Last year, China had introduced new rules to limit the amount of time minors spend on online games with an objective to combat gaming addiction.

TikTok continues to face the heat over safety and wellbeing of minors on its platform. In the US, a bipartisan coalition of state attorneys in the US has launched a nationwide investigation into TikToks effect on the mental health and wellbeing of children. In UK a High Court judge has permitted a class-action style privacy lawsuit to proceed against TikTok over its handling of children's data. The suit, which was filed in December 2020, is seeking damages on behalf of children for unlawfully processing children's data, breaking UK and EU data protection law.

Anti-Trust

Big tech continue to be under the radar of regulators across the globe.

In China market regulator State Administration of Market Regulation (SAMR) has tightened its scrutiny over livestreaming e-commerce platforms. The SAMR expressed concerns of misleading advertisements by internet influencers and advised live-streaming platforms to conduct self-inspections to ensure product quality and if necessary punish livestreamers who sell inadequate products.

The U.S. House Judiciary Committee has asked the Department of Justice to probe Amazon for "potentially criminal conduct" amid competition probe.

In India the Competition Commission of India (CCI) is arguing to restart probe over alleged preferential treatment given by Amazon to sellers.

The South African Competition Commission has referred Meta to a tribunal over alleged abuse of its dominant market position.

EU and UK plan to open antitrust probe into a 2018 deal between Google and Meta and in EU Microsoft faces antitrust complaint about its cloud computing business.

Privacy and Data Protection

In terms of fine for privacy breach, this month Irish data regulator has imposed a 17 million euro ($18.7 million) fine on Meta after an inquiry into 12 data breach notifications the regulator received in 2018.

A new research has found Google to be collecting data about calls and text messages through its Android operating system.

Australian watchdog has sued Meta for failing to failed to prevent scammers to promote fake ads on its platform.

App stores

Regulators across the world are involved in lawsuits or interventions over the dominant market position of the two app platforms -Google and Apple.

South Korea has passed a new law, an amendment to the Telecommunication Business Act, allowing the government to ban app stores of companies such as Apple and Google from forcing software developers to use their payments systems. The rule was enforced on 15 March. According to the guidelines, any in-app store operator who mandates use of a certain payment system, face the risk of a fine of up to 2 percent of its sale. The guidelines suggest that app market operators with more than 100 billion won ($81.3 million) in app market service revenue in the previous fiscal year, more than a daily average of 1 million users will "face higher possibility" of being applied to the new rule as they are deemed as having superior status over app developers. All three app market operators – Google, Apple, and One store – fall in the category.

In the Netherlands, Apple is facing a Dutch class- action lawsuit that alleges app prices higher owing to Apple's commissions and that the total cost to consumers is almost €5 billion.

In France, the Finance Minister has informed that both Google and Apple will be sued over "abusive" contractual terms imposed on startups and developers on their platform and seek fines of 2 million euros ($2.5 million). Further, Google has been fined €2 million by the Paris Commercial Court over abusive behaviour against developers in its app store. The Court ordered Google to amend seven clauses from its contract dating back to 2015 and 2016.

Investigations by the Competition Commission of India (CCI) has found Google Playstore billing guidelines to be 'unfair' and 'discriminatory'. As the next step CCI will be hearing the matter, post which it may release its ruling.

Other Updates:

- Israel launched first Quantum computer
- Intel announced and initial investment of over €33 Billion for R&D and manufacturing next generation semiconductors in EU. €17 billion will be invested in a 'leading-edge semiconductor fab mega-site' in Germany, dubbed the 'Silicon Junction'. Intel will also expand its existing fab in Ireland, invest in a 'state-of-the-art back-end manufacturing facility' in Italy, create a new R&D and design hub in France, and invest in R&D, manufacturing, and foundry services in Poland and Spain.
- U.S. Senate approves $52 billion chips bill in bid to reach compromise
- The UK's Financial Conduct Authority (FCA) has warned operators of cryptocurrency ATMs in the UK to down their ATM services
- Internal emails acquired by the Washington Post indicate that Meta hired prominent US consulting firm Targeted Victory to work on shifting public opinion against TikTok by spreading information that the platform is dangerous for children and society in America. Defending the company, a spokesperson from Meta stated 'We believe all platforms, including TikTok, should face a level of scrutiny consistent with their growing success.'
- Twitter, Vimeo; Automattic the parent company of WordPress.com, WooCommerce, Tumblr; Seznam; and Jodel, have founded an new advocacy group e Open Internet Alliance (OIA) to influence European digital policy and beyond through "Fair" regulation
- China's new financial court the Beijing Financial Court will handle lawsuits involving overseas firms and protect the interests of domestic investors. This comes at a time when Chinese firms are being targeted by the US government with sanctions.
- ZTE has been summoned for a hearing to a U.S. federal court in Texas in a case where the Chinese telecommunications equipment maker is accused of violating probation in connection with an alleged conspiracy to commit visa fraud.
- Brazil high court revoked ban on Telegram after it blocked disinformation accounts a few days after Brazil's Supreme Court suspended Telegram.

Updates from India

- Reserve Bank of India has banned Paytm Bank from onboarding any new customer. The bank has been directed to get a comprehensive IT audit conducted by an external IT audit firm and conduct a comprehensive audit of its IT system conducted, Basis the report, and after a go ahead of the regulator, the bank will be able to onboard new customers. Paytm on its part has refuted the claims of leaking data to Chinese firms terming them to be "false and sensationalist". It is reported that PayTM is still to appoint an external audit firm to conduct the audit of its IT systems.

- The Standing Committee on Communications and Information Technology has expressed concern on high spectrum price and delay in 5G rollout. The committee reiterated that the Department of Telecom needs to review all their policies relating to 5G so that the country is not left behind in the 5G race.

- The Karnataka government plans to approach supreme court to overturn the Karnataka High court order and ban online games with real money stake.

- The Amazon & Future battle intensify deepens. Last month we reported that both parties were working on an out of court settlement. It is reported that Amazon demanded $200 Million that it had invested in Futures as settlement while Future suggested that it had no funds and Amazon can take a stake in a group firm. However, the talks failed and Amazon has gone ahead and attacked Future and Jio accusing them of fraud in Indian newspaper. In a letter Reliance has defended its takeover of Future outlets stating it kept Future **“**out of harm’s way” with financial support.

- Jaideep Misra, Joint Secretary MeitY has been appointed Vice Chair, Government Advisory Council (GAC) at ICANN.

- ITU's Standing Council Standing Committee has appointed Aprajita Sharrma as Vice-Chairperson. She will remain as vice-chairperson of the Council Standing Committee for the years 2023 and 2024 and its chairperson in 2025 and 2026.

ICANN Updates

ICANN73

ICANN73 Policy Forum was organised online between 7-10 March. More than 1,570 attendees from 146 countries participated in 79 sessions. There were two plenary sessions: on The Global Public Interest Framework: Is it Useful? and Evolving the DNS Abuse Conversation. Apart from bilateral meetings between different SOs/ACs different SOs and ACs had their own meetings. For more details read the ICANN73 Outcome report**.**

ICANN Updates

In March , ICANN CEO provided an update on ICANN's Emergency Internet Infrastructure Support Initiative of $ 1 million USD to support Internet access and that the first distribution would be in Ukraine. The ICANN Board Chair shared highlights from March ICANN Board Workshop
ICANN enacted relief for registrants in Ukraine and surrounding region; published, the Draft Planning Prioritization Framework Version 1 which is available here; a report The Last Four years in Retrospect: A Brief Review of DNS Abuse Trends**;** provided update on the UNR Registry Agreement Assignments Status

ICANN is seeking inputs on: Uniform Domain Name Dispute Resolution Policy (UDRP); Root Zone Update Process Study; Root Zone Label Generation Rules Version 5

APAC DNS Forum 2022

The APAC DNS Forum 2022 themed “Beyond Technology: The Revolution of DNS”, was co-hosted by MYNIC and ICANN online from 29 March - 1 April. The event was inaugurated by the Honorable Deputy Minister of the Ministry of Communication and Multimedia Malaysia, YB Datuk Zahidi Zainul Abidin.

Discussions at the forum ranged from the future of Domain Name System (DNS), Internationalized Domain Name (IDN) Variants; protecting domain names from Cybersquatters and Counterfeiters; issues related to DNS Abuse including efforts to mitigate such abuse; think or thin registry and data escrow, digital branding, emerging technology, privacy issues, best practices, etc.

Upcoming events: 8th Middle East Domain Name System (DNS) Forum will take place virtually from 16-18 May 2022

Upcoming webinar: Webinar on issues impacting the Internet that are being discussed at the United Nations (U.N.) and the International Telecommunication Union (ITU) on 12 April at 20:00 UTC. To participate register here.

ISOC Updates

ISOC has been actively speaking why the Internet infrastructure should not be broken. In that context, this month ISOC published two Internet Impact Briefs on Network Refusals and on Ukraine's Requests to ICANN and RIPE NCC, as well as a quick analysis overview**.** Chair of ISOC Board of Trustees released a statement why the Internet should not be partitioned.

Applications are invited from members for the Mid-career Fellowship till 4 May. Register here.

The Call for Nominations for 2022 Jonathan B. Postel Service Award is open until 13 May.

APNIC Updates

APNIC announced that APNIC54 will be a hybrid conference from 8-15 September in Singapore. APNIC will also be co-hosting AprIGF and APSIG meetings during that time.

Apart from routine activities in March, APNIC participated in several events including ICANN, WTSA, IETF and vPhNOG 2022 to name a few. For more updates on APNIC read the APNIC Blog.

The application for 2022 ISIF Asia Grants is now open. For more details, please read the Opportunities section.

TRAI Updates

In March, TRAI initiated a pilot study at Delhi International Airport for Next Generation Telecom Infrastructure deployment using street furniture; issued Telecom Tariff (67th Amendment) Order, 2022; issued Consultation Paper on Use of street furniture for small cell and aerial fiber deployment and Rating of Buildings or Areas for Digital Connectivity; extended comment/ counter-comments period on consultation paper on Promoting Networking and Telecom Equipment Manufacturing in India to 1st April and 18th April.

TheTelecom Subscription Data report of January 2022 released by the regulator, indicates a drop in telecom subscribers from previous month (1178.41million in December 2021) to 1169.46 million and broadband subscribers to 783.43 million from 792.08 million in December.

Upcoming Open House Discussions (OHDs) in April:

Ease of Doing Business in Telecom and Broadcasting Sector on 21 April and Promoting Local Manufacturing in the Television Broadcasting Sector on 28 April.

Other Updates

Articles & Reports:

- UNESCO, the Inter-American Development Bank (IDB) and the Organisation for Economic Co-operation and Development (OECD) have released a report "The effects of AI on the working lives of women" that examines the effects of the use of AI on the working lives of women.
- CUTS International and CUTS Institute for Regulation and Competition (CIRC) have published their annual India Competition and Regulation Report 2021: Towards Inclusive Digital Economy in a post-COVID era
- CUTS has released a discussion paper Impact of Criminalising Provisions on Ease of Doing Digital Business in India

Events:

- World Telecommunication Standardization Assembly(WTSA-20) was held between 1-9 March in Geneva, Switzerland. The draft proceedings of meeting is available here.
- BIF organized a Panel Discussion on 11 March on 'Unpacking social & economic gains from Encryption'. The speakers in the panel were: G Narendra Nath, National Security Council Secretariat, Government of India; Prof. Debayan Gupta, Ashoka University; Robin Wilton, Internet Society; and Raman Jit Singh Chima, Access Now.
- IETF113 was organized from 19 -25 March.
- MediaNama organised a members call on Russia-Ukraine War: Impact on the Internet on 22 March the presentation is available here.

Upcoming Events & Opportunities

Upcoming Events

- INNOG5 will be held online between 3 to 6 May. 3 and 4 will be workshops and 6 will be conference.
- 11th edition of RightsCon will be held online from 6-10 June.
- ICANN74 Policy Forum Meeting is scheduled to be held in The Hague, Netherlands from 13 to 16 June.
- AprIGF will be held in September in Singapore.
- APNIC54 will be held 8-15 September in Singapore.
- ICANN75 Annual General Meeting is scheduled for 17–22 September in Kuala Lumpur, Malaysia.

Opportunities

- Nominations are invited for the Pandit Deendayal Upadhyaya Telecom Skill Excellence Award 2022 by 15 April
- There is a call for papers for INNOG5 by 24 April. For more details visit this link.
- There is a call for proposal for APrIGF 2022. The overarching theme this year is: PEOPLE AT THE CENTRE: *Envisioning a community-led Internet that is inclusive, sustainable and trusted*. Details of the overarching theme and the thematic tracks can be found here. Last date to submit proposal is 28 April. For more details visit this link.
- Applications are invited from ISOC members for the Mid-career Fellowship till 4 May. Register here.
- The Call for Nominations for 2022 Jonathan B. Postel Service Award is open until 13 May 2022. The award from Internet Society commemorates Jon Postel's extraordinary stewardship in the course of his 30-year career in networking.

- Applications for the 2022 ISIF Asia Grants is now open till 15 May. Applications are invited from public and private sector organizations, academia, non-profits, and social enterprise organizations on three thematic areas: Inclusion, Infrastructure and Knowledge. Read here for more details.

CCAOI, C/o AWFIS, L 29-34, Above Haldiram, Connaught Place, New Delhi - 110001.
Visit us online at: www.ccaoi.in
If you wish to unsubscribe from this newsletter or for any comments/suggestions email: info@ccaoi.in