MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE
Liberté
Égalité
Fraternité

Direction générale du Trésor

REVUE DE PRESSE SECTORIELLE

NUMERIQUE

UNE PUBLICATION DU SERVICE ÉCONOMIQUE REGIONAL

DE NEW DELHI

N° 4 –20 au 30 Avril 2021

En bref

NUMÉRIQUE :

- Atos acquiert le canadien Processia, le britannique Ipsotek et l'allemand Cryptovision après l'échec du rachat de l'américain DXC technology.
- L'Australie et l'Inde annoncent un programme conjoint de recherche sur l'IA, la 5G, l'internet des objets et l'informatique quantique.
- La RBI interdit à American Express et Diners Club International de recruter de nouveaux clients en Inde au nom du non respect de la localisation des données.
- Le gouvernement indien ordonne à Twitter et Facebook de censurer les messages critiquant la gestion de la crise de la COVID-19.
- Multiplication des attaques informatiques chinoises contre les infrastructures critiques indiennes.

TÉLÉCOMMUNICATIONS:

- L'internet satellitaire semble promis à un bel avenir en Inde.
- OneWeb a levé 550 millions de dollars auprès de l'opérateur de satellites français Eutelsat Communications pour une participation de 24 %.
- L'Inde pourrait atteindre 820 millions d'utilisateurs 4G cette année, avec une intensification de la couverture du pays.

Revue de presse

1. NUMÉRIQUE

Atos makes three more acquistions while reporting a drop in revenue

Reuters, 20/04/2021

Gdansk, Poland: Atos SE has acquired three more companies as the French IT consulting group continues its series of bolt-on acquisitions while reporting a drop in its first-quarter revenue.

The Atos Group said Tuesday that it had bought Canada-based Processia, UK-based Ipsotek and German cybersecurity firm Cryptovision. It gave no financial details of the transactions, and said the deals were expected to close in the second and third quarters.

Atos completed in 2020 a series of bolt-on acquisitions in a bid for its mid-term revenues to reach a 65% share in digital, cloud, security and decarbonisation.

In February, Atos and US rival DXC Technology decided to discontinue talks about what would have been the deal-hungry IT consulting group's biggest acquisition to date, worth more than $10 billion.

The Paris-based firm, which develops end-to-end solutions in hybrid cloud, big data, business applications and digital workplace said its first-quarter revenue came 1.9% below last year's figure at €2.69 billion ($3.24 billion). Earlier in April, it disclosed that auditors had found accounting errors at those units, leading the shares to slump 18%. Atos confirmed its full-year guidance of revenue growth of 3.5% to 4% and an operating margin of between 9.4% and 9.8%.

The group said it has decided to conduct a full accounting review of the two US legal entities and would give a status update at the time of first half results on July 28.

Australia and India team up on critical technology

TechTarget, 22/04/2021

Australia and India have joined hands to advance the development of critical and emerging technologies such as artificial intelligence (AI), 5G networks, the internet of things (IoT) and quantum computing through a research grant programme.

Through the programme, the two countries hope to “help shape a global technology environment that meets Australia and India’s shared vision of an open, free, rules-based Indo-Pacific region”.

The first three projects in the initial round of the programme, which prioritised proposals focused on strengthening understanding of ethical frameworks and developing technical standards for critical technologies, were recently announced by Australia’s department of foreign Affairs and trade.

This project, led by the Centre for International Security Studies at the University of Sydney and experts such as Rajeshwari Rajagopalan of the Delhi-based Observer Research Foundation and quantum physicist Shohini Ghose, aims to develop quantum accords to shape international governance of quantum technologies.

The team will build guiding principles on ethics, best practices and progressive applications of quantum technologies.

But rather than propose a formal set of universal rules, they will seek consensus among key stakeholders on what constitutes ethical or unethical behaviour, good or bad practices, productive or destructive applications for emerging quantum technologies.

The project, spearheaded by La Trobe University and Indian Institute of Technology Kampur, will provide Australian and Indian business with an ethics and policy framework when outsourcing their technology to Indian providers.

It will do by improving the understanding of how they translate being signatories of ethical codes to their actual

practice. The project will also analyse the emotions and views of stakeholders expressed in social media on the ethical issues found to be important through business surveys.

In doing so, the project intends to advance knowledge in AI and cyber and critical technology, ethics and sustainability and risk by bringing together disciplines in business management and ethics, computer science and engineering, and AI and business analytics.

The outcomes expected include recommendations on revised ethical codes and practices and a framework for using AI and advanced analytics to review ethical practices of companies.

5G privacy and security

The explosive growth in wireless network usage and IoT systems is expected to accelerate. While 5G networks offer significant improvements in terms of capacity, data rates, and potential energy efficiency, there is a need to address critical privacy and security challenges.

The work will focus on the issues that arise from wireless tracking systems that rely on detecting variations in the channel state information (CSI) due to the users' physical activities and wireless networking.

Based on a series of experiments in Australia and India, the project will develop a comprehensive understanding of the extent of private information and metadata exposed and related inferences. This will be used to engage with standards and regulatory agencies and government bodies to strengthen data protection regimes in Australia, India and globally.

The research will be the basis for a whitepaper detailing the emerging wireless network privacy and security threat landscape. This will be followed up with a workshop in Bangalore with key regulators, standards body officials, policy makers and researchers, with the goal of initiating action to effectively address the emerging threats.

The work will be led the University of Sydney, University of New South Wales, Orbit Australia, Reliance Jio Infocomm, Indian Institute of Technology Madras and Calligo Technologies.

RBI restrains American Express Banking Corp., Diners Club International from onboarding new customers

The Hindu, 23/04/2021

The Reserve Bank of India has imposed restrictions on American Express Banking Corp. and Diners Club International Ltd. from onboarding new domestic customers onto their card networks from May 1. "These entities have been found non-compliant with the directions on storage of payment system data. This order will not impact existing customers," the Reserve Bank said on Friday.

American Express Banking Corp. and Diners Club International Ltd. are payment system operators authorised to operate card networks in the country under the Payment and Settlement Systems Act, 2007 (PSS Act).

The supervisory action has been taken in exercise of powers vested in RBI under Section 17 of the PSS Act.

As per the terms of RBI circular on Storage of Payment System Data of April 6, 2018, all payment system providers were directed to ensure that within a period of six months the entire data (full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction) relating to payment systems operated by them is stored in a system only in India.

They were also required to report compliance to RBI and submit a board-approved system audit report (SAR) conducted by a CERT-In empanelled auditor within the timelines specified therein.

Meanwhile, American Express in a statement said, "We have been in regular dialogue with the Reserve Bank of India about data localisation requirements and have demonstrated our progress towards complying with the regulation. While we're disappointed that the RBI has taken this course of action, we are working with them to resolve their concerns as quickly as possible. This does not impact the services that we offer to our existing customers in India, and our customers can continue to use and accept our cards as normal."

India orders Twitter and Facebook to takedown posts critical of its coronavirus handling

Techcrunch, 24/04/2021

Twitter and Facebook have taken down about 100 posts in India, some of which were critical of New Delhi's handling of the coronavirus, to comply with an emergency order from the Indian government at a time when South Asian nation is grappling with a globally unprecedented surge in Covid cases.

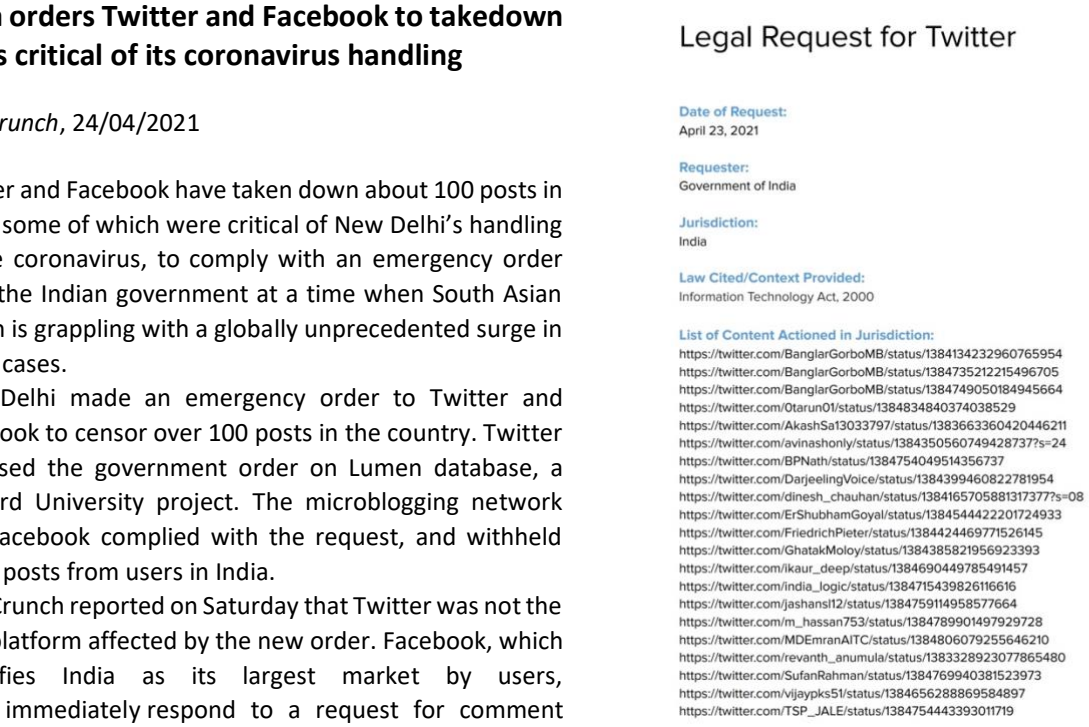
New Delhi made an emergency order to Twitter and Facebook to censor over 100 posts in the country. Twitter disclosed the government order on Lumen database, a Harvard University project. The microblogging network and Facebook complied with the request, and withheld those posts from users in India.

TechCrunch reported on Saturday that Twitter was not the only platform affected by the new order. Facebook, which identifies India as its largest market by users, didn't immediately respond to a request for comment Saturday.

The Indian government confirmed on Sunday that it ordered Facebook and Instagram and Twitter to take down posts that it deemed posed potential to incite panic among the public, hinder its efforts to contain the pandemic, or were simply misleading.

(Credit where it's due: Twitter is one of the handful of companies that timely discloses takedown actions and also shares who made those requests.)

The world's second largest nation — which has also previously ordered Twitter to block some tweets and accounts critical of its policies and threatened jail time to employees in the event of non-compliance — comes as the country reports a record of over 330,000 new Covid cases a day, the worst by any country. Multiple news reports, doctors, and academicians say that even these Covid figures, as alarmingly high as they are, are underreported. Amid an unprecedented collapse of the nation's health infrastructure, Twitter has become a rare beam of hope in what it describes as one of its "priority markets" as people crowdsource data to help one another find medicines and availability of beds and oxygen supplies.



Legal Request for Twitter

Date of Request:
April 23, 2021

Requester:
Government of India

Jurisdiction:
India

Law Cited/Context Provided:
Information Technology Act, 2000

List of Content Actioned in Jurisdiction:
https://twitter.com/BanglarGorboMB/status/1384134232960765954
https://twitter.com/BanglarGorboMB/status/1384735212215496705
https://twitter.com/BanglarGorboMB/status/1384749050184945664
https://twitter.com/0tarun01/status/1384834840374038529
https://twitter.com/AkashSa13033797/status/1383663360420446211
https://twitter.com/avinashonly/status/1384350560749428737?s=24
https://twitter.com/BPNath/status/1384754049514356737
https://twitter.com/DarjeelingVoice/status/1384399460822781954
https://twitter.com/dinesh_chauhan/status/1384165705881317377?s=08
https://twitter.com/ErShubhamGoyal/status/1384544222201724933
https://twitter.com/FriedrichPieter/status/1384424469771526145
https://twitter.com/GhatakMoloy/status/1384385821956923393
https://twitter.com/ikaur_deep/status/1384690449785491457
https://twitter.com/india_logic/status/1384715439826116616
https://twitter.com/jashansl12/status/1384759114958577664
https://twitter.com/m_hassan753/status/1384789901497929728
https://twitter.com/MDEmranAITC/status/1384806079255646210
https://twitter.com/revanth_anumula/status/1383328923077865480
https://twitter.com/SufanRahman/status/1384769940381523973
https://twitter.com/vijaypks51/status/1384656288869584897
https://twitter.com/TSP_JALE/status/1384754443393011719

A copy of one of Indian government's orders disclosed by Twitter. (Lumen database)

Policy-focused Indian news outlet Medianama, which first reported on New Delhi's new order Friday, said among those whose tweets have been censored in India include high profile public figures such as Revanth Reddy (a Member of Parliament), Moloy Ghatak (a minister in West Bengal), Vineet Kumar Singh (actor) filmmakers Vinod Kapri and Avinash Das.

In a statement, a Twitter spokesperson told TechCrunch, "When we receive a valid legal request, we review it under both the Twitter Rules and local law. If the content violates Twitter's Rules, the content will be removed from the service. If it is determined to be illegal in a particular jurisdiction, but not in violation of the Twitter Rules, we may withhold access to the content in India only. In all cases, we notify the account holder directly so they're aware that we've received a legal order pertaining to the account."

"We notify the user(s) by sending a message to the email address associated with the account(s), if available. Read more about our Legal request FAQs. The legal requests

that we receive are detailed in the bianual Twitter Transparency Report, and requests to withhold content are published on Lumen."

India has become one of the key markets for several global technology giants as they look to accelerate their userbase growth and make long-term bets. But India, once the example of an ideal open market, has also proposed or enforced several rules in the country in recent years under Prime Minister Narendra Modi's leadership that in some ways arguably makes it difficult for American firms to keep expanding in the South Asian market without compromising on some of the values that users in their home market take for granted.

China's state-sponsored hackers are targeting India's infrastructure. And silence may not be golden.

ET Prime, 26/04/2021

On April 8, in an address to the Vivekananda International Foundation, India's topmost defence officer made a comment that prompted strategic-affairs experts to sit up and take notice.

India's Chief of Defence Staff, General Bipin Rawat, in a rare admission, said, "We know that China is capable of launching cyberattacks on us, and that can disrupt a large amount of our systems."

Rawat said that the "biggest differential" between India and China lies in the field of cyber domain, adding that China has been able to invest a lot of funds on new and disruptive technologies.

Experts termed it unprecedented.

Lukasz Olejnik, a Europe-based independent cybersecurity researcher and advisor tells ET Prime, "The recent disclosure by India concerning the weakness of India when it comes to cyber defence was very interesting, such announcements are very rare. Perhaps, it may help in convincing the public to allocate more funds on cyber defence, and so perhaps this was the goal behind this speech."

It surely is unprecedented. This was the head of India's Integrated Defence Staff (IDS) speaking. IDS has representations from all of India's premier institutions whose aim is to preserve national security at any cost.

Later, at the Raisina Dialogue, on April 15, Rawat took things a notch higher. He said, "Unconventional means of conflict being employed by clever use of disruptive technologies could paralyse networks, causing breakdown of systems like banking, power grids, transportation, and communication to name a few."

Though Rawat's comments were unprecedented, India has already seen a precedent, as he was pointing at, not too long ago.

On October 12, 2020, when India's financial capital Mumbai was busy battling Covid-19 and was beginning to see some success, it all went black.

The city suffered from a massive power outage that left its lifeline — the railways — the stock market, and several hospitals out of options in the middle of it all.

For cyber defence -affairs experts, the Mumbai incident was reminiscent of what happened in 2015 in Ukraine — the first known successful cyberattack on a power grid. The state-sponsored hackers compromised information systems of critical civil infrastructure of three energy-distribution companies in the eastern European country and temporarily disrupted the electricity supply to consumers for hours.

Strategic-affairs observers believe that Chinese state-sponsored actors have been trying to influence the status quo at the line of actual control (LAC) and improve the bargaining position of China's People Liberation Army (PLA) by the use of hybrid warfare technologies, including cyberwarfare tools on India. All of this is being done without using kinetic military force.

Juxtaposed with the multiple rounds of commander-level talks at the LAC in the last 11 months without much progress, Chinese state-affiliated hacking groups have dug deep to disrupt India's critical information infrastructure (CII).

According to multiple third-party cyber-security firms, a wide range of India's CII remains vulnerable. Key assets such as power grids to IT infrastructure of vaccine makers appear to be on the agenda of the Chinese state-sponsored hacking groups.

These groups from China are well-known for continually challenge the existing geopolitical order. This is done alongside prompting a direct conflict at the border. These state-linked actors are usually known to be operating in the expanding grey area between war and peace. The ease with which they are able to attack key systems questions India's cyber-preparedness with respect to China.

US-based cybersecurity firm Recorded Future, which studies the use of the Internet by state actors, traced Mumbai's power-outage incident in October to a hacking group called Red Echo, affiliated with the Chinese government, as discovered in a recent report.

A total of 21 IP addresses linked to 12 Indian organisations in the power-generation and transmission sector — classified as critical — were targeted.

In denial?

Close on the heels of the Recorded Future report, the power ministry said that prompt action had been taken and there was "no impact" on any of the facilities caused by the "referred threat".

Union power minister RK Singh denied reports of a Chinese cyberattack leading to a power outage and said it was found to be a 'human error' based on reports submitted by multiple teams.

Recently, Telangana's state-run power utility claimed to have thwarted a potential Chinese-origin cyberattack on its systems after an alert from the Computer Emergency Response Team of India (CERT-In), the country's nodal agency to deal with emergency cybersecurity threats.

Recorded Future did mention Telangana State Load Despatch Centre as one of the organisations targeted by Red Echo in its report.

Another Singapore-based cybersecurity firm, Cyfirma, warned India of a possible cyberattack by China-affiliated hacking groups — Gothic Panda and Stone Panda.

Gothic Panda is a long-standing Chinese threat actor group, which has targeted the aerospace, defence, construction and engineering, high tech, telecommunications, and transportation/manufacturing sectors in the past.

Stone Panda is another Chinese threat actor group, which has traditionally shown interest in stealing international trade secrets and supply-chain information from various enterprises across many countries such as India, Japan, the US, Canada, and Brazil.

Security experts believe that the two are directly connected to the Chinese Ministry of State Security's (MSS) Tianjin bureau.

In February, Goldman Sachs-backed Cyfirma said that IT systems of two Indian vaccine makers whose coronavirus shots are being used in the global immunisation campaign, were being targeted.

It said that Chinese hacking group APT10, also known as Stone Panda, had identified gaps and vulnerabilities in the IT infrastructure and supply-chain software of Bharat Biotech and the Serum Institute of India (SII), the world's largest vaccine maker.

From power grids to vaccine makers. And there's more.

In an internal government note in March, CERT-In advised the transport and highways ministry stating that it had, "...observed continued target intrusion activities from Chinese state-sponsored actors, directed towards the Indian transport sector with the possible intention of collecting intelligence and conducting cyber espionage aligned with the national strategic goals of the Chinese national policy priorities."

Entities like IRCTC, Tata Motors, NHAI, RITES, Dedicated Freight Corridor Corporation of India, CRIS, Andhra Pradesh's roads and building department were subject to cyberattacks during the period between May 2020 and February 2021.

In the past and even now, Indian military experts have repeatedly warned successive governments about reliance on Chinese power and telecom equipment and how it would turn into a major security risk for the country.

Strategic-affairs expert Brahma Chellanay agrees. “Today, India faces serious cyber-sabotage risks. It must cut dependencies on China for critical equipment.”

The dragon’s expanding cyber arsenal

According to the Belfer Center for Science and International Affairs’ National Cyber Power Index, with evidence collected from publicly available data, China is second only after the United States in the index of most comprehensive cyber powers.

The Belfer centre made this determination by utilising an index that measures cyber capabilities of 30 countries in the context of seven national objectives, using 32 intent indicators and 27 capability indicators.

As per the index, China’s cyber objectives have been linked to not just surveillance and control, but also for commercial purposes.

The report states that China conducts regular industrial espionage with an aim to incentivise and grow its domestic cyber expertise through research and development, and public-private partnerships.

It adds that China also uses its cyber power for not just active defence purposes but also for offensive capabilities.

People's Liberation Army Strategic Support Force (PLASSF) is well known as the cyber, space, and electronic warfare services branch of the PLA.

PLA has a close relationship with private Chinese telecommunication companies and the ‘patriotic hackers’ are its arsenal.

PLASSF's outreach programme under its civil-military integration enables it to engage universities, private software industries, and ‘patriotic hackers’. This was outlined in a key policy document by Cyberspace Administration of China.

“The PLASSF has gradually cultivated a very refined cyber doctrine pivoted upon the concept of non-contact operations. This is a step above asymmetric warfare and a different beast altogether which the Indian military doesn’t fully understand,” Pukhraj Singh, cyber defence expert, tells ET Prime.

Singh adds, its “positional defence, mobile offense” for concept and “three attacks, three defence” for doctrine requires a crucial deconstruction. The said doctrine lays a very heavy emphasis on cyber operations and cyber-electromagnetic activities.

Olejnik also points out, “China has one of the best defensive and offensive cyber teams in the world, this is clear. I would expect China has full readiness when it comes to offensive cyber capabilities. We just did not see them.”

Words of Olejnik and Singh are a big black box for India, represented by the barrage of frequent attacks.

India’s lack of preparedness is China’s gain

India’s lax cyber preparedness was recently exposed, yet again.

Ethical-hacking group from the US, Sakura Samurai, uncovered a large number of critical vulnerabilities in the Indian government’s system recently.

"We found 34 pages of vulnerabilities in less than 24 hours on the Indian government systems. Based on our findings, it was apparent that Chinese attacks wouldn’t even have to be complex to be able to take advantage of India's poor cybersecurity posture. A lot of projects and access-control restrictions are non-existent," US-based hacker and founder of Sakura Samurai, John Jackson, tells ET Prime.

The group ethically hacked into over a dozen Indian government organisations and reported their findings to the National Critical Information Infrastructure Protection Centre (NCIIPC) in February of this year.

“Our youngest hacker, Jackson Henry (15), along with his friend Zultan Holder, initiated the hacks of the Indian government’s key assets,” Jackson says.

“Once Henry and Holder began to uncover some of the vulnerabilities, Robert Willis, Aubrey Cottle, and I jumped on the project and began to help. Subsequently, the additional teamwork allowed for a rapid discovery of a massive amount of exposures on a wide range of state assets. Outside of the discovered credentials and other sensitive information, Willis found exposed police records

and forensic data and Henry noted 14K+ exposed user records," Jackson adds.

"As a final test of defense, I performed Remote Code Execution, which allowed me to completely control the Government of Kerala's local self government's financial server. This gave me unfettered access to financial records, and Aubrey Cottle exploited the vulnerability further, chaining together my vulnerability with his own session takeover vulnerability, resulting in full access to the financial application itself - with the ability to take over anyone's account or perform critical actions on their behalf," he elaborates.

As per exclusive data shared with ET Prime by the hacking group, following Indian government organisations were found with exposed directories for projects containing sensitive credentials and data:

1.Government of Bihar

2.Government of Tamil Nadu

3.Government of Kerala

4.Telangana State

5.Maharashtra Housing and Development Authority

6.Jharkhand Police department

7.Punjab Agro Industries Corporation Limited.

List of Indian government organisations with files exposing their credentials, SMS service, recaptcha keys and secrets:

1.Government of India, Ministry of Women and Child Development.

2.Embassy of India, Tehran

3.Embassy of India, Bangkok, Thailand

4.Government of Delhi, Department of Power GNCTD.

List of Indian government entities with exposed private keys:

1.Competition Commission of India

2.Government of Goa, Captain of Ports department.

3.Government of West Bengal, Directorate of Pension, Provident Fund and Group Insurance.

4.Government of Chennai, The greater Chennai Corporation etc.

India's multiple weak nodes

When it comes to cybersecurity, India has multiple weak spots seen with the capabilities that China has developed over the years.

There are several areas where India needs to strengthen itself, for instance:

1.India suffers from a poor allocation for a cyber defence budget.

2.India's cyber defence command is still in a nascent stage even after two years of its announcement.

3.India is still heavily dependent on China for telecom and power equipment.

4.Public-private partnership in defence is absent in cyber-defence technologies. Unlike China, where some of the top private companies work with Chinese government's strategic cyber-defence programmes.

5.India is still relying on help from foreign nations to build capacities rather than fortifying existing infrastructure to create cyber resilience.

Even after 11 months, the two nuclear-armed neighbors, India and China, are caught-up to resolve the pending boundary issue on LAC.

At the same time, India's poor cyber-defence posture is giving China an upper hand in the utilisation of hybrid-warfare techniques through its state-sponsored actors.

In May 2018, the UK became one of the first countries to set out its legal approach to applying international law in cyberspace.

As the future battle lines are redrawn with cyber warfare taking the centre stage, India should look at following the UK's model of applying international law in cyberspace.

Of the 29 countries with cyber strategies, 27 countries noted their pursuit of Defining International Cyber Norms and Technical Standards in their strategy.

India and Egypt did not participate in the definition of a good defence posture. India's first cybersecurity strategy document is still to see the light of day even as China's blatant cyber warfare persists and intensifies during the pandemic.

The bottom line

India's top strategic allies, the US and the UK, formally attributed the supply-chain attack of IT infrastructure-management company, SolarWinds, with "high confidence" to government operatives working for Russia's intelligence service, Foreign Intelligence Service (SVR).

India needs to become more transparent when addressing various cyberattacks even if they are from state-sponsored hackers from across the border on India's CII's.

The government should ensure that the RVDP or Responsible Vulnerability Disclosure Program, run by NCIIPC, should be given due cognizance to encourage ethical hackers to check on the vulnerable CII infrastructure.

With China being a leader in both offensive and defensive cyber capabilities, having an effective laid out cyber-deterrence strategy will be a shot in India's arm. An effective defence is only half the war won.

As Sun Tzu said, "Invincibility lies in the defence; the possibility of victory in the attack."

Another power-grid outage fueled by Chinese hackers amid the Covid-19 pandemic can get India gasping for breath within minutes. New Delhi can't relax.

2. Télécommunications

No wires or towers: Satellite broadband promises to be the next big thing in India

ET Telecom, 25/04/2021

It is super-fast and does not need wires or towers to connect to the world wide web. Satellite broadband promises to be the next big thing and a slew of big names are ready to roll it out as early as next year, reports ET's Kalyan Parbat.

Imagine sitting in a remote mountain village north of the Rohtang Pass in Himachal Pradesh and chatting with colleagues in Delhi or Bengaluru over an uninterrupted video call. Or, watching a Clint Eastwood western on a laptop in the Andamans – without using a cellular network or wired broadband.

This may soon turn into a reality once satellite broadband connections are rolled out across India, likely as early as next year.

Some of the biggest global names – including OneWeb, SpaceX and Hughes - are betting big on the opportunity to deliver satellite-based fast internet services - anywhere, anytime.

OneWeb, co-owned by Bharti Global and the UK government, is launching high-speed satellite internet services in the country by mid-2022.

Tech billionaire Elon Musk's SpaceX Technologies is looking to do the same next year with a maze of satellites.

Hughes Communications India, the local arm of US satellite maker Hughes Network Systems, is also ready to invest in a $500 million satellite and pump in $300 million more on ground-level gear to deliver such connectivity.

Star wars

There is growing buzz around satellite broadband and the far-reaching implications of the internet-from-space race.

"The future is probably shifting now. If you extrapolate this 10 years from now, will there be ground networks at all?

Who knows?" Bharti Enterprises chairman Sunil Mittal told ET in a recent interaction. "Every month you will see a launch; we need to send 650 satellites; they will go up by April 2022. Then, we'll be up and running. This will be nothing but telecom in space."

OneWeb is in constant touch with the Indian Space Research Organisation (Isro) and regulators to ensure all approvals for market access and landing rights are in place before it goes live in India, Mittal's UK-based son Shravin, the managing director of Bharti Global and the one responsible for driving the group's satellite business, told ET separately.

SpaceX is already offering a beta version of its Starlink satellite internet service on pre-orders.

This comes with a refundable deposit of $99 (more than Rs 7,000) in India.

The Starlink beta service has even been opened up for pre-orders to potential customers in remote trans-Himalayan zones such as the Keylong-Leh road in the high-altitude Lahaul valley.

Once operational, the beta version alone will pack data speeds of 50-150 Mbps, which will increase sharply once more satellites are put into orbit, according to Starlink's website.

So, why are these marquee names keen to enter the satellite broadband business in a country with a 63% reach of 4G services and one of the lowest mobile data rates in the world?

While existing telecom networks have largely delivered broadband connectivity to consumers in urban and suburban areas, industry experts say the Covid-19 pandemic painfully revealed how millions in India's rural and remote corners still do not have access to fast internet or reliable mobile connections.

"SpaceX's Starlink high-capacity, high-speed, low-latency satellite network would advance the goal of delivering broadband connectivity to all Indians, particularly those without access now or in the near-term to broadband services, traditionally available only to customers in urban and suburban areas," said Patricia Cooper, VP (satellite government affairs) of SpaceX, responding to the Telecom Regulatory Authority of India's paper on broadband speeds.

Nearly 75% of India's rural population do not have access to broadband since many locations go without cellular or fibre connectivity, according to the estimates of the Broadband India Forum (BIF), which represents OneWeb, Hughes, Amazon, Google, Facebook, Microsoft and Qualcomm.

Hence, powerful next-generation satellite systems are being touted as a viable alternative to connect the unconnected.

One reason why the likes of OneWeb and SpaceX are "attracted to the new stirrings in India's satellite broadband space is that satellite networks can be rolled out and scaled up a lot faster and more cost-effectively than terrestrial mobile/broadband networks, especially to connect a sizable chunk of the population living in remote and inhospitable regions," says Mahesh Uppal, a telecom analyst and director of Com First (India).

Satellite internet players also do not have to worry about securing right-of-way clearances which typically slow down terrestrial broadband network rollouts.

Last year, finance minister Nirmala Sitharaman said the government would create a level-playing field for private satellite builders, satellite launchers and space-based service providers under its new space communication policy, which would ring in a predictable regulatory regime.

Once the 'Open Space' policy is fully operational, satellite broadband services can be a $500 million-plus near-term market opportunity, the Satcom Industry Association (SIA-India) says.

At present, satellite broadband services in India are a primarily B2B play with a market size of roughly $100 million.

Satellite broadband is a key connectivity solution – for banks with numerous branches in remote areas where mobile coverage and wired internet are unreliable or even small and medium enterprises operating in far-flung regions.

The biggest potential money spinner - in a B2B scenario - is to use satellites to boost mobile broadband coverage in rural areas where there is not enough mobile towers or terrestrial backhaul links via fibre networks, industry executives point out.

“We believe satellite broadband can provide the vital ‘backhaul’ or connectivity between mobile towers and a telco’s core mobile network in rural areas to ensure uninterrupted mobile coverage in such regions,” K Krishna, vice president and CTO at Hughes Communications India, told ET.

The revenue opportunity is significant.

Each remote tower would need at least 20 Mbps to deliver cellular backhaul via satellite.

Since every Mbps of satellite connectivity can garner an average revenue per user (ARPU) of Rs 16,000-Rs 20,000 a month, the potential monthly ARPU for a satcom operator providing such connectivity in a remote area can be as much as Rs 3.2-Rs 4 lakh per month.

Prohibitive costs

However, satellite broadband will not see mass consumer traction like mobile services unless satellite internet rates crash.

At present, these services are priced at around $15-$20 per GB in India, about 22-30 times higher than the $0.68 charged per GB for mobile data.

There are several reasons why this is so.

Satcom operators in India have no access to high-throughput satellites offering 100-500 Gbps of bandwidth. This is because most conventional satellites (with low transponder capacity) are run by Isro and offer only a maximum 12 Gbps. These are largely reserved for government programmes, hampering commercial satcom services.

Satcom players also cannot lease bandwidth capacity directly from foreign satellite operators.

They have to go via the Department of Space (DoS), which pushes up final leasing costs by around 15-20%, including a withholding tax component.

“Hughes provides satellite broadband services to consumers in many markets, but for this service to be viable and successful (in India), the input cost of capacity has to be substantially lower than what it is today,” Krishna says.

Current leasing costs “are in the range of Rs 75,000 per Mbps per month, which is 10 times the global average of Rs 7,500,” he says.

The rates will fall sharply only if a satellite service provider is able to control every cost element, like in the mature satellite markets.

In the United States, satellite companies like SpaceX, Hughes or Viasat own, operate and launch satellites. They also directly deliver satellite internet services to consumers. This is akin to telcos who buy spectrum, roll out networks and offer mobile services.

In India though, the case is different.

A potential satellite broadband operator will first need to lease bandwidth at a higher cost through DoS. They will then have to separately seek a VSAT permit from the Department of Telecommunications (DoT) or enter into a third-party pact with an existing VSAT permit-holder before offering satellite internet services. Multiple intermediaries end up hiking the cost of services.

Further, bandwidth leasing agreements are only for a year or less despite a satellite’s 15-year lifespan. This artificially increases costs due to the uncertainties around foreign satellite capacity utilisation, making satellite broadband rates unaffordable.

Industry experts say such leasing contracts should be for a minimum of three years. India’s dependence on foreign satellite operators will not disappear overnight, they say, since Isro satellites meet only around 50% of the country’s needs.

India is working on building high throughput satellites -- offering more than 100 Gbps bandwidth capacity -- but there are no timelines yet.

"There is an insatiable demand for broadband connectivity, but there simply isn't enough domestic satellite capacity to serve this growing demand in India," says Anil Prakash, director general, SIA-India.

Isro did not reply to ET's detailed queries, while questions to OneWeb and SpaceX also went unanswered.

Pricing of satellite broadband services can plunge to as little as $1 per GB -- on par with global rates -- if satcom operators can directly lease bandwidth from foreign operators and access very high-throughput satellites.

Going forward, satellite broadband can become the backbone for networks of Internet of Things (IoT) devices, smart factories, utilities and other systems that require complex machine-to-machine communications, according to brokerage CLSA.

The satellite industry is also hopeful that the government may allow 100% foreign direct investment through the automatic route.

The industry though is wary of DoS's current combined role as licensor, market regulator and satellite operator. This, they say, is leading to a conflict of interest with private satellite makers and satcom service providers.

In its recent submissions to the government on the draft satcom policy, the VSAT Services Association of India has suggested that DoS's role should be segregated.

BIF is also of the view that DoS must only evaluate proposals for authorisation of satellite capacity. It should not be a party in commercial contracts between satellite operators and service providers, it says.

Bharti-backed OneWeb to raise $550 million from France's Eutelsat

ET Bureau, 27/04/2021

Kolkata: Bharti Group-backed OneWeb is raising $550 million (Rs 4,103 crore approx) by selling a 24% stake to French satellite operator, Eutelsat Communications, bringing its total funding to $1.9 billion, and helping it inch closer to launching a first-generation satellite fleet, totalling 648 satellites next year.

Eutelsat, a geo-stationary satellite operator, will be a significant equity partner and enjoy similar governance rights to the UK government and Bharti Global, who co-own OneWeb. Bharti Global is the overseas arm of Bharti Enterprises -- the holding company of Bharti Airtel, India's second-largest telco. The investment is expected to be completed in the second half of 2021, subject to regulatory approvals, OneWeb said in a statement Tuesday.

"…as an open multi-national business, we are committed to serving the global needs of governments, businesses and communities across the world," Bharti Enterprises chairman Sunil Mittal said in the media statement.

Mittal, who is also OneWeb's executive chairman, added that "together we are stronger, benefitting from the entrepreneurial energy of Bharti, the extensive global outreach of the UK government and the expertise in the satellite industry of Eutelsat.

Bharti Airtel shares closed 1.31% higher at Rs 534.45 on BSE Tuesday. The OneWeb deal was announced late evening, post-market hours.

Back in January, SoftBank Group and Hughes Network Systems LLC had together pumped $260 million into OneWeb.

The latest big-ticket funding comes even as OneWeb prepares to deliver high-speed, low-latency satellite broadband services in rural and remote regions globally (including India), aiming to take on the likes of Elon Musk's SpaceX and Jeff Bezos's Amazon-linked Project Kuiper. OneWeb is slated to roll out satellite internet services in India by June 2022.

OneWeb's partnership with Eutelsat is slated to enhance "both companies' commercial potential, leveraging Eutelsat's established commercial reach to governments and enterprise customers in addition to its strong institutional relationships, recognised technical expertise and global fleet," the companies said in the joint statement.

OneWeb's CEO Neil Masterson said the company "now has 80% of the necessary financing" for the Gen 1 fleet, of which nearly 30% is already in space. He added that Eutelsat's global distribution network advances the market entry opportunities for OneWeb, which looks forward to working together to capitalise on the growth opportunity and accelerate the pace of execution.

Eutelsat's CEO Rodolphe Belmer, in turn, said the French satellite operator is "excited to become a shareholder and partner in OneWeb" in the run up to its commercial launch later in the year, adding that it is "confident in OneWeb's right-to-win, thanks to its earliness to market, priority spectrum rights and evolving, scalable technology".

Last November, Bharti Global MD Shravin Mittal had told ET that OneWeb is open to entering India either directly or through a commercial partnership, involving either the JV route or a bandwidth capacity leasing pact, even as it gears up to launch fast broadband services in the country by June 2022.

Earlier this month, Nettle Infrastructure Investments, a wholly-owned arm of Bharti Airtel, acquired 100% stake in OneWeb India Communications Pvt Ltd, in an all-cash deal for an undisclosed sum. Airtel, in an exchange filing this month, had said that UK-based Network Access Associates Ltd, a OneWeb group company, was in the process of seeking foreign direct investment (FDI) approval for investment in OneWeb India Communications Private Ltd.

India's 4G user base may grow to 820 million in FY22 as telcos expand coverage: Crisil

ET Bureau, 27/04/2021

India's 4G user base is slated to grow to around 820 million in FY22 despite a Covid spike as competition is set to intensify with the Big 3 telcos likely to use their freshly acquired airwaves to boost coverage and push the country's remaining 250-to-300 million feature phone users to go 4G, said Crisil Research.

The ratings agency said "India's 4G subscriber additions in FY22 will be more than in the last fiscal, despite the Covid19 second wave". This, due to higher competitive intensity stemming from significant spectrum acquisitions by the big telcos in the March 2021 auction, leading to "Bharti Airtel, Reliance Jio and Vodafone Idea achieving spectrum parity in terms of the Mhz/million subscriber metric".

In a bull scenario, Crisil estimates the 4G user base rising to 820 million by end-FY22, assuming Covid restrictions last only for the April-June quarter. But even in a bear case, where lockdowns get extended through the second quarter, it estimates the 4G user base reaching 800-810 million, well above the estimated 710-720 million level in end-FY21.

The ratings agency also expects Airtel and Vi to step up efforts to migrate their 2G/3G customers to 4G to reduce their network operating costs, especially as revenue inflows from interconnect usage charges (IUC) have disappeared since January. More so, since both incumbents have refarmed their 3G airwaves for 4G use across a majority of their circles, leading to significant 4G capacity addition.

Crisil expects the Big 3 operators to focus this fiscal on gaining and upgrading the 250-300 million feature phone users to go 4G.

"With the recent spectrum acquisition, telcos are well-positioned to handle any surge in data traffic, leading to increased aggression by the players to gain market share," the ratings agency said in a research report.

In the 4G spectrum auctions that ended on March 2, Jio picked up 488.35 units of spectrum in 22 circles across India in the 800 Mhz, 1800 Mhz and 2300 Mhz bands for Rs 57,123 crore. Airtel acquired 355.45 units across the 800 Mhz and 900 Mhz bands, besides the 1800 Mhz, 2100 Mhz and 2300 Mhz, for Rs 18,699 crore. Vi bought only 11.8 units in five circles for Rs 1,993.4 crore that it needed to beef up its 4G holdings.

Crisil, however, expects the nature of competition among the big telcos to be indirect, in the form of "tie-ups with smartphone makers for low-cost phones, increased bundling of over the top (OTT) content and lower entry points for upgrade customers".

Crisil expects neither Jio nor Bharti Airtel "to bite the bullet and raise tariffs" as the top two players are running neck and neck on active subscriber market share. Active or

`visitor location register' (VLR) data, put out by the Trai, is a key metric that reflects the actual number of customers actively using a mobile network. As per Trai data, Airtel and Jio's active user market shares were 33.7% and 33.6% respectively in December 2020.

La direction générale du Trésor est présente dans plus de 100 pays à travers ses Services économiques.
Pour en savoir plus sur ses missions et ses implantations : **www.tresor.economie.gouv.fr/tresor-international**

MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE
Liberté
Égalité
Fraternité

Responsable de la publication : Service économique de New Delhi
Rédacteurs : Feli VISCO

Pour s'abonner : Contacter le SER de New Delhi
Crédits photo : ©DG Trésor