CYFY
THE INDIA CONFERENCE ON CYBER SECURITY AND INTERNET GOVERNANCE

ORF CYBER MONITOR

CYFY 2015 14th to 16th October

VOLUME III | ISSUE 6 | JUNE 2015 | http://cyfy.org

COMMENTARY

Strive for Balance without Surrendering Net Neutrality

Mahima Kaul

India's Telecom Regulatory Authority has looked to other countries for best practices on how to deal with the issue of net neutrality. What is the best way forward?

Is India Contemplating Net Neutrality Regulation Prematurely?

Manoj Kumar

The net neutrality debate has caught up with India, proving to be a controversial issue pitting internet service providers against end users. Over-the-top services are a particular concern in the country.

India and the System behind the Internet of Things

Anahita Mathai

The Internet of Things (IoT) is already revolutionising the global digital space. What does the draft Indian IoT policy mean for programmes like Digital India and the smart cities initiative?

New World Information Order, Internet and the Global South

Branislav Gosovic

More than four decades ago, the Non-Aligned Movement launched the concept of a New International Information Order. It could be time for that concept to re-emerge and the world debates internet governance.

Why Smart Cities Need to Get Wise to Security – and Fast

Nicole Kobie

The smart city is an alluring vision of the future, but security researchers warn that they could become more vulnerable to hackers than today's computer systems and smartphones.

The Observer Research Foundation's monthly round-up of the biggest stories making international headlines in cyberspace.

ESSENTIAL READINGS

STATEMENTS

Turn to Page # 19

EDITORIAL

Governance

The French parliament has approved a new bill granting intelligence agencies "sweeping new surveillance powers", including tapping phones and reading emails without prior permission from a judge. Telecom companies and internet service providers will be required to produce user data on request. France's national assembly passed the bill by 438 votes to 86, despite opposition from leftwing and green members of parliament to several provisions of the bill. These include the mass collection of metadata, bugging homes, logging keystrokes and the retention of such data for up to five years. International civil liberties organisations like Amnesty International have described the bill as 'intrusive' and have campaigned against it. The bill, which was pushed through in part because of the Charlie Hebdo attacks, is now under review by the French senate.

Meanwhile in the USA, while efforts to extend the Patriot Act were fruitless, the Senate also failed to pass the US Freedom Act, which would severely curtail the spying powers of the National Security Agency (NSA) – in particular the mass collection of telecom data. Among other provisions, the bill required the NSA to go to court before it can access phone records, which will be retained by telecom companies. Support for the bill was not universal, as some felt its language was too weak and did not address critical transparency and oversight issues. However, it did pass in the House of Representatives, which decided voted 338-88 in its favour.

Net neutrality may become part of licensing conditions for telecom service providers in India, with Indian Minister for Communications and Information Technology Ravi Shankar Prasad saying that options were open regarding how to proceed on the issue of net neutrality. The minister also said that privacy ought to be safeguarded, following an incident where the country's telecom regulatory authority released published the email addresses associated with every response to their consultation paper on net neutrality – more than a million in total. The Competition Commission of India, which had started investigating unfair practices amongst internet service providers, has decided to wait for the government to issue guidelines or regulations before taking the matter further.

Civil society groups in India have also been reacting to India's comments on the Internet Assigned Numbers Authority (IANA) transition. India responded to the second draft proposal of the Cross Community Working Group to Develop an IANA Stewardship Transition Proposal on Naming Related Functions, expressing concern about the role of ICANN and pushing for greater accountability.

Microsoft announced a radical change in the way it will take forward its Windows operating system (OS). At the company's Ignite conference, held from May 4-8, 2015, a developer said that "Windows 10 is the last version of Windows", prompting speculation that Microsoft may be retiring the OS. It quickly became clear that the plan instead was to revamp the system and introduce "Windows as a service". The new system would involve rolling updates and improvements to the system, in the same way that mobile applications are constantly upgraded, rather than a full overhaul every few years.

Crowd-funding is underway for a new computer which will be sold for less than 10 dollars. Created by Next Thing Co, the CHIP is considerably smaller and cheaper than its famous competitor the Raspberry Pi. The CHIP offers a full desktop experience but its low cost means that some features are sacrificed; for example adding HDMI or VGA video capability increases the price of the device considerably. Nevertheless, the CHIP signals that computing could soon become much cheaper.

The path of free speech in Bangladesh took a turn for the ominous and tragic with the killing of blogger Ananta Bijoy Das, a rationalist and blogger. Das, who was 32, is the third blogger to be killed in Bangladesh in the last 4 months; all of them had posted pieces online that were deemed to be "critical of Islam". While Al-Qaeda in the Indian Subcontinent has claimed responsibility for Das' killing, several have linked it to a hit list published last year by a group called the Defenders of Islam. Of the 84 names of that list, nine have been killed, and several others attacked. Rights groups have criticised Dhaka's response to the attacks, calling it inadequate.

The decisions made by Google in response to user Right to be Forgotten requests are being challenged in the UK by the Information Commissioner's Office (ICO). The ICO handles complaints from users who are unhappy with the way Google has dealt with their requests; it has so far found that in 75 percent of cases so far, Google has acted properly. Nevertheless, the system of challenges and checks highlights the difficulty of responding to such requests.

As the digital currency Bitcoin becomes more popular, more efforts are made to regulate it. Perhaps in a sign of things to come, Xapo, which provides vaults for Bitcoin, is moving from California to Switzerland. Wences Casares, the company's founder and CEO, laid out the reasons for the move in a statement; they included Switzerland's international reputation in finance, regulatory stability, neutrality and the fact that the company's servers were located in that country. Analysts have speculated that another reason for the shift is that Switzerland affords more privacy for Xapo's customers, and other companies could follow suit as countries like the USA ponder digital currency regulation.

Security

Nearly 10 percent of the most popular HTTPS-protected sites are vulnerable to hacking and surveillance due to a flaw named LogJam. The flaw is a result of US regulations from the 1990s, which prevented exported versions of US software from maintaining the same level of encryption as those used domestically. Though it seems that thus far the flaw has not been exploited by hackers, finding a workable solution has proved complicated. Employing the best fix for the bug could result in access to up to 20,000 websites being blocked while their security remains in doubt.

NATO has for the first time deployed underwater drones as part of a research testing. Drones are expected to be more widely used by navies around the world in their efforts to scan ocean beds. In particular, drones may prove useful in transmitting information which can help submarines distinguish between shipwrecks, natural formations and other obstacles underwater as well as tracking moving objects like others submarines, warships and torpedoes. Scientists at NATO's Centre for Maritime Research and Experimentation have noted that using unmanned technology like drones is advantageous as it eliminates much of the danger to humans while transmitting an unrelenting stream of real-time information. They expect that within five years, drones will become a standard part of NATO military exercises.

Several countries in Africa are taking steps to counter the rising threat of cybersecurity breaches on the continent. In particular, the South African government has promised to finalise their national cyber security policy within the current financial year. They had previously been criticised for delaying the rollout of the policy. The International Telecommunication Union's planned regional centre for cyber security will most likely be based in Rwanda, a country which has undertaken extensive efforts to boost its own cyber capabilities.

Russia and China have inked a cybersecurity deal which analysts suggest could lead to deeper cyber cooperation between the two nations. Apart from agreeing not to use cyber attacks against each other, the two countries have also pledged to exchange technology and information through law enforcement agencies. They have also stated their intention to "jointly counteract" certain types of technology which could disrupt public order and interfere with the stability of their domestic political, social and economic environments. The pact has led some to suggest that the emergence of an "alternative internet", excluding

the US, is inevitable, and would be a major threat to freedom of speech online. Part of this concern arises from US suspicions that a cyber breach that affected its Internal Revenue Service originated in Russia, and from its longstanding tension with China over cyber attacks. For its part, China is preparing a five-year "cybersecurity plan to protect state secrets and data", which also encourages the use of domestic hardware – which could hamper the business of foreign tech firms operating in the country.

China is not the only Asian country to undertake a cyber cooperation agreement this month. Singapore's Cyber Security Agency signed a memorandum of understanding, its first, with the French Agence Nationale de la Sécurité des Systèmes d'Information. The two countries have agreed to "strengthen collaboration" by sharing best practices and expertise and by increasing the number of bilateral exchanges held. Additionally, India has signed a cybersecurity agreement with Mongolia as part of an ongoing relationship that has recently been elevated to a "strategic partnership".

In an effort to thwart Islamic extremists online, the US is taking forward cooperation with Gulf Cooperation Council states. Apart from tackling the threat posed by the Islamic State, the new cooperation agreement will focus on other actors in the Gulf region, including Iran. Tehran is a particular concern for both the US and its Gulf allies like Saudi Arabia, which blamed Iran for an attack on its major oil company, Saudi Aramco.

Strive for a balance between access & price, without surrendering on network neutrality principles

Mahima Kaul

The TRAI consultation paper on Regulatory Framework for Over-the-top (OTT) services 2015, certainly revealed a few biases by asking what India could learn from ETNO or best-practices from other countries at the end of Chapter 4 on Regulatory Interventions for OTTs in Other Countries. ETNO, or the European Telecommunications Network Operators, put out a plan in 2012 to enable European telecom operators to negotiate pricing schemes with OTT providers. This included OTTs paying 'fair compensation for traffic', new models to provide Quality of Service, and non-interference by governments in such arrangements between the network operators and information services. The price of popularity would be settled privately, without intervention by the regulator in negotiations.

This chapter in the TRAI paper then goes on to summarize the regulatory frameworks and best practices from around the world. Briefly, these offer three distinct models: the first, offers separate regulatory regimes for communication services and non – communication services, as in the case of Germany and France. The second model is based on the use of price discrimination on traffic to ensure development of broadband infrastructure, as is followed in the UK and Korea. And finally, the third model that prescribes, a 'fair, reasonable, and non-discriminatory' approach to deal with regulatory issues, such as is the practice in Korea or with ETNO.

Thus, it would appear that the question seems to be asking, Should TRAI regulate OTTs or allow telecom companies to negotiate directly with OTTs service providers on the issue of charging them for growing data traffic? Surprisingly, however, there is another model that has been spelt out in Chapter 4, but oddly, is absent from the list of Queries at the end. This is the model which the USA is attempting to chart out for themselves, i.e.: 'bright-line rules' for the internet which includes principles of 'no blocking, no throttling, and no paid prioritization' of data. In the US, 'Reasonable Network Management' is allowed, but the ISPs must ensure that network management have legitimate aims and are not used to provide 'unlimited data' or other anti-network neutrality practices.

Since the TRAI has looked to other countries for ideas and inspiration for developing an Indian model, it is fair to first examine the market that is being addressed. India has 12-15% internet penetration, with further rise expected via mobile phones. Today the country has 140 million smartphones, which are getting cheaper to buy, by the day, and 687 million GSM phones in rural areas. The internet is a vehicle of growth; outside of the acknowledged popularity of VoIP services, there is also the expectation that e-commerce will fuel internet growth as well. E-commerce generated sales of $16 billion in 2014, while overall the retail industry in India is valued at around $600 billion. Additionally, the government's 'Digital India' initiative is also expected to fuel traffic; in fact, it already has in rural areas. Reports indicate that the first half of 2014 has seen 3.5 billion electronic transactions, of which 1.7 billion transactions were related to e-governance projects. 35% of these transactions came from rural areas. Broadly stated, content, commerce and e-governance will be drivers of the internet in India as much as infrastructure, availability of electricity, connectivity, access and pricing will be.

If one ignores the telecom arguments for paid prioritization and examines whether schemes like zero-rating would help promote internet penetration, a different set of questions emerge. Is it better for citizen-consumers to have access to some limited sites free of cost than to have no

access at all? Can zero-rating, in some ways, be compared with "free sampling", following which users might want to experience the larger internet? And, could paid prioritization packs be designed to become 'Digital India' packs, which could contain part commercial data, part news data, and part socially and locally relevant and useful data, thereby helping rural citizens to access both free content and also use e-governance apps at no cost? The answers cannot be simple, and perhaps they cannot be effectively answered by those who have no problem in paying monthly internet bills.

These questions are intriguing. A few years ago, internet users may remember, the expectation of users was that all content on the internet would be free. Some bigger brands attempted to start content-subscription based models, but actually, an advertising-based model today supports most of the freely available content. Internet users also pay for free content by surrendering their data. Ultimately, an innovative, even if a morally ambiguous model emerged, wherein consumers were connected to advertisers, which enabled 'free' content.

And this is when we start examining 'free' access that comes with its own caveat. Allowing citizen-consumers to access only certain websites for free, could over the long term, end up creating 'walled gardens' – a term which denotes a closed ecosystem in which the carrier or service provider has control over applications, content, and media, and restricts convenient access to non-approved applications or content. This goes against the principle of free and open qualities that have made the internet the tool it is today – an engine for economic growth and innovation. In fact, given that only those platforms which can afford to pay for prioritization would be offered for free, the entire exercise has an anti-competitive angle to it. And it must be noted that the conversation in India is looking at internet service providers breaching the network neutrality principle of 'paid prioritization' as opposed to a conversation about internet 'fast lanes' which have fuelled arguments in the US about preserving network neutrality.

If Indian ISPs were to offer varying degrees of speed to sites in a market already struggling with internet speeds, it would certainly mean that smaller and newer OTTs would be simply defeated by the internet wheel of time. Could this mean that the market leaders of today would simply institutionalize their leadership online, or could fundraising models for all future apps necessarily have to account for 'zero-rating' or 'fast-lane' charges?

So what should India do, going ahead? Create two competing versions of the internet; between those who would like to access the full spectrum of internet sites and those who would rather subscribe to digital packs which offer a few products at a zero-rating? Would this fulfill the government's aim to achieve 50 crore internet connections by 2018, or is this what it means to have a 'Digital India'? The Minister for Communications and IT has called the internet 'the finest creation of human mind and it does not encounter any boundary and it does not get stopped by geography," adding that it "must be owned by the entire mankind, not by a few."

Perhaps, India should seek to strive for a balance between access and price, without surrendering on the network neutrality principles. Shouldn't the telecom operators wait to see what new streams of revenues would develop for them as the internet grows in India? Shouldn't companies be able to promote their brand in the country, but compromising on the key principles that has so far set the internet apart from other mediums of communication? And finally, shouldn't people have a clear understanding of what the hidden costs of "free" really is, and if they are willing to pay for it?

One lakh emails to the regulator aside, this conversation is certainly not over. Ironically, what it has done is encourage 1 lakh people to engage with the bureaucracy, in a democratic system, by actually sending in their comments to the TRAI consultation paper. Now, imagine, if you didn't even know about this because your internet pack only focused on cricket and movie songs?

The author is Head of the Cyber and Media Initiative at ORF.

This article originally appeared on Thinking Aloud! May 2015

Is India Contemplating Net Neutrality Regulation Prematurely?

Manoj Kumar

The seemingly inevitable net neutrality [NN] debate has finally caught up with India. Borne of the clash of interests between Internet Service Providers [ISPs] and the users of their services, NN has been a controversial issue in countries with significant markets for the internet for some time now. The duelling factions each have compelling arguments to support their cases, and though present here in some measure already, deliberations over what are deemed "over-the-top" [OTT] services used over telecommunication network bandwidths, have been kick-started in earnest by the furore around the recent Airtel Zero – Flipkart deal [that the latter has withdrawn from in the face of rising criticism][1]. This has led to the release of a consultation paper on the subject by the Telecom Regulatory Authority of India [TRAI][2]that seeks to create a regulatory infrastructure around network services, which has drawn widespread flak from civil society and opposition leaders.

Definitions

To understand the vagaries of an issue with such far-reaching repercussions as this, it is important to develop a conceptual understanding of what the terms 'net neutrality' and 'over-the-top services' mean. According to Tim Wu, the American jurist popularly considered to have coined the term, net neutrality-

"**decrees that internet service providers must treat all traffic equally, and let users do what they wished with their bandwidth**."[3]

According to TRAI's definition, NN can be construed to mean that -

"**.. TSPs must treat all internet traffic on an equal basis, no matter its type or origin of content or means used to transmit packets. All points in a network should be able to connect to all other points in the network and service providers should be able to deliver traffic from one point to another seamlessly, without any differentiation on speed, access or price.**"[4]

In essence, this implies that once a user pays for the use of bandwidth, it should be theirs to do with as they choose, and that the network company should not dictate the terms of the user's engagement with the net. As for OTTs, in the TRAI's own words -

"**The term over-the-top (OTT) refers to applications and services which are accessible over the internet and ride on operators' networks offering internet access services e.g. social networks, search engines, amateur video aggregation sites etc.**"[5]

What is the significance of NN in India?

Net neutrality here has emerged as an issue on mobile networks rather than their fixed line counterparts. Given the internet's rate of growth in India - the number of mobile internet users is set to reach a total of 223 million by June 2015 [according to a report by the Internet and Mobile Association of India and IMRB International (a market research firm)] - it might be argued that it is not too early to develop a framework to govern OTT apps; policies and regulations that can be updated as the market expands. The government must be careful though, to keep from imposing any debilitating regulation upon an infrastructure that is still finding its feet. Restricting

[1]http://economictimes.indiatimes.com/tech/internet/flipkart-pulls-out-of-airtels-net-neutrality-violating-airtel-zero/articleshow/46916966.cms
[2]http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/OTT-CP-27032015.pdf
[3]http://www.wired.com/2014/06/tim-wu/
[4]http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/OTT-CP-27032015.pdf
[5]http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/OTT-CP-27032015.pdf

existing users' access to any assortment of services might have the effect of negatively impacting untapped markets, especially considering that the domestic market's capacity has not been fully realized. Even so, this argument may have been rendered redundant by the fact that TRAI has already decided against additional regulation for mobile value-added services which in practical terms might categorized in the same strata of services as are OTT apps.

What, then, is the importance of the internet, and why has it inspired such agitation about its management? The answer lies in the web's genesis: The internet was imagined as a public resource and therefore created in the image of a vast "commons", a repository of human knowledge and information; in playing this role successfully, the net has transformed the nature and exchange of ideas, and become a vital, ever-expanding organism more critical to free speech in our status quo than any other medium of communication. To block, modulate or circumvent access to the internet at this stage in its evolution would negate the very rationale of the net's existence.

The question must be asked however –is blocking off or circumscribing access to the internet in any manner the government's intention in this case? While it has been alleged that the TRAI's consultation paper is but a part of a lobbying exercise by big telcos to promote their interests, a closer examination of the issue reveals that circumstances as they exist in India do not support such a standard of service as NN envisages without adequate bandwidth and the network outages and congestion that are part of the Indian internet experience. Already with the rapid growth in users, an unprecedented load is placed on existing networks - in such a case, it makes little sense to forward time insensitive data at the same priority as real-time voice or video traffic. In both the Indian scenario and in a global context, this skewed view of how internet works and the call for net neutrality by disregarding concerns for efficiency can lead to impeding the development of infrastructure.

Arguments Against and For Regulation

Another point of discussion in the current debate is centred on the loss of revenue caused to telecommunication companies due to the rapidly increasing use of OTT services such as popular instant messaging applications [WhatsApp, Snapchat, Google Talk], e-commerce sites [Flipkart, Amazon], video aggregation and sharing [YouTube, Vimeo, Netflix], etc., which have come to span almost the entire spectrum of the web, and all of which consume significant amounts of bandwidth without having to share their earnings with the ISPs that establish the infrastructure through which they operate.[6] It is these services that have come under the purview of regulatory authorities in order to decide on alternative revenue-sharing models, such as those proposed by Airtel Zero.

Before taking any steps towards the regulation of OTT services however, those in charge must consider their rationale in the prevailing context, and that of the internet in the broader scheme of things: it is to connect as efficiently as possible, the users of these facilities, creating a network to enable communication and exchange of information in a manner unprecedented in history, and with enormous repercussions to the exchange and cultivation of ideas; a neutral internet supports free speech, democratic participation, and empowers citizens. By facilitating permission-free innovation at the edges of the network, it ensures robust competition amongst service providers. Then there is of course harnessing the benefits of the net for education, health care, and the society at large - the power of a tool with the capacity to penetrate geo-political borders as the web does, is integral to the development process.

As stated above, broadband connectivity in India is very low at present, and there is a huge need [and potential] for increased network creation. The next huge wave of internet users will be arriving mostly armed with low-end smart phones; it is imperative to keep in mind here that this dynamic creates a different relationship to the

[6] http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/OTT-CP-27032015.pdf

internet from traditional connections at home or work. In such a scenario, licensing OTT services, as the TRAI has in its consultation paper proposed to introduce, will have the obvious impact of a drop in existing users due to an increase in the prices of such services, possibly also alienating markets that have not even been tapped yet. The combination of increased costs and the monopolistic powers of ISP might make it more difficult for low-cost innovation to sustain itself, something that the internet has been especially valuable in fostering since its inception. The idea, then, of strict regulation is one which could be put in storage till such time that India has achieved increased access.

No debate can be complete without affording both sides a chance to present their cases, and it cannot be denied that those advocating for regulation of the net and its supplementary services, have some legitimate reasons to back their demands. To begin with, there is the service providers' right to ease congestion caused by heavy bandwidth consumption services [for example, YouTube] by discriminating in bandwidth distribution. It is a fact that neutrality can come in the way of the growth of quality services, when elastic applications in the nature of peer-to-peer file sharing or video sharing platforms are likely to crowd out quality-sensitive services due to congestion. This does not have to have negative connotations -benefits are optimized in a network organization in which quality of service differentiation is acceptable as long as it serves a reasonable purpose and discrimination is avoided. In determining which behaviours are tolerable and which are not, regulators should be looking at not whether the practice is unfair, but rather at the potential harms, such as the extortion of rents, tying and bundling, etc.

Users can select intelligently the mobile products and services suited to their budget; if users feel zero rated programs are discriminatory, they can simply choose not to buy them – it is not uncommon to see operators failing due to lack of consumer interest. It is obvious that telecom companies should not be allowed to engage in illegal discriminatory activity, but some commentators have pointed out that neutrality proponents are displaying a troubling pattern of wanting to eschew existing law [such as the Competition and Information Technology Acts] in favour of inventing new laws and increasing regulatory burden.

In what could be another important point in favour of regulation, the TRAI paper mentions OTT service providers fall under the Indian telecom licensing regime whereas TSPs operate under a separate regime wherein voice and messaging services can be offered only after obtaining a license. TSPs have claimed that many OTT services are similar in nature to what the TSPs have been catering to, but remain unencumbered by the licensing agreements that the TSPs have to abide by while providing those services. In doing this, OTT service providers essentially piggyback over the infrastructure provided by the TSPs, which enables them to offer similar services at drastically lower costs. As a result, there is the absence of a level playing ground for the two competing products same consumer services segment. Thus, it would be worthwhile to reorganize the services provided by OTT service providers in terms of the consumer services segment they cater to, rather than blindly classifying them as data services.

Comparative Neutrality Regimes

In February this year, the Federal Communications Commission [FCC], being the nodal regulatory authority in the US, brought into force the Open Internet Rules [OIR] which classify ISPs as "common carriers", rendering them equivalent to telecom service providers. In January 2014, a federal appeals court had struck down the FCC, which in 2010 had introduced provisions preventing internet service providers from blocking websites or imposing limits on users. Consequently, a user created a petition on White House's 'We the People' platform, leading up to the installation of the OIR.

The debate has taken a different shape in the European Union, with strong restrictions on privacy and traffic management. The current policy proposal is one that essentially prohibits traffic management on the public Internet. In 2013, the Commission introduced a legislative proposal "Connected Continent: Building a Telecoms Single Market" – Intended to end

discriminatory blocking and throttling and deliver effective net neutrality.[7][8]

However, it is how things unfold in the developing world may have a bigger impact on the future of the Internet. Worldwide, the number of smart phones is projected to double from 1.5 billion last year to three billion in 2017. Most of those 1.5 billion new phones—and new Internet access—will be in the developing world. India, despite its low consumer penetration, will have an important role to play in this expansion, and it will be interesting to see how the government faces up to the challenge of reconciling the varied interests of service providers and consumers.

In a major indication of the shift in internet user demographics, countries with developing economies have been amongst the first to bring in net neutrality law. Chile, recognized as one of the more advanced telecom markets in Latin America, outlawed zero rating services in 2014, banning operators from offering free access to social media websites as part of a mobile data package and including provisions for parental controls, privacy, virus protection, and network security. In this course, it became the first Latin-American country to implement net neutrality laws. Nearby Brazil, too, passed a legislation called the "**Internet Bill of Rights**" last year, which makes equal access to internet mandatory - ISPs are barred from restricting content and from charging more for data-heavy services - and protects the privacy of the Brazilian internet users.

In India, which has a market similar to Brazil and Chile's in terms of penetration and affordability of services, the concept of net neutrality has no basis in law: the TRAI has made attempts at establishing neutrality rules several times before this but to no avail as yet. However, there exist several legislations, including the Indian Penal Code, the Code of Criminal Procedure, the Indian Telegraph Act, the Indian Telegraph Rules, and the Information Technology Act and its supplementary rules, that can be used to govern the internet. Also, all telecom services available in the country are subject to regulatory provisions, if not in particular, then at the very least in generic legislation.

The author is a Managing Partner at Hammurabi & Solomon.

[7] https://gigaom.com/2014/04/03/european-parliament-passes-strong-net-neutrality-law-along-with-major-roaming-reforms/
[8] http://www.bbc.com/news/technology-26865869

India and the System behind the Internet of Things

Anahita Mathai

The Internet of Things (IoT) is already revolutionising the global digital space. The Asia-Pacific region is set to become a hotspot; by the year 2020, it is estimated that there will be some 8.6 billion 'connected' devices in the area. In line with this estimate, analysts project the market to grow to over 580 billion US dollars – a figure which is likely to be even higher when the numbers for Japan are factored in. 20 percent of those 8.6 billion devices will be in China, home to the largest population of internet users in the world. However, while the largest IoT market may end up being China, it is not considered the most 'mature' market. Calculating market maturity based on connections per capita, or the number of connected devices compared to a country's population, the International Data Corporation suggests that South Korea is in fact the most mature of the Asia-Pacific markets. In anticipation of this growth and the regulatory challenges it may pose, countries are trying different tactics to keep pace. India's Department of Electronics & Information Technology, under the Ministry of Communication and Information Technology, has gone so far as to release a Draft Policy on the topic.

India's policy defines the IoT as "an interplay for software, telecom and electronic hardware industr[ies]" which has great potential. Already there are nearly twice as many connected devices as there are people on the planet. India's planned IoT policy aligns with other major projects of the government, including the Smart Cities project and the Digital India programme. The Internet of Things will not only feed into those projects, but itself be developed further as they progress. Given the implications of a smoothly-running IoT network for sectors like disaster management, health, security, energy and agriculture, the goal of the Indian government is to create an IoT network that is "connected, secure and smart".

For the purposes of the IoT policy, the 'system' underlying the Internet of Things has been divided into three areas: technology, analysis and decision making. The first stage, technology, represents one end of the network, with sensors and devices collecting information and eventually performing tasks. Much of the public consciousness around the Internet of Things comes from wearable devices and household items that are connected to the internet. These include 'fitness devices' which measure physical exertion, sleep and other activities; smart watches and other technologies which sync with phones; and items like Google Glass which incorporate several of these elements. However, the aforementioned technologies all involve humans in direct contact with devices. Increasingly remote devices are being developed and it is very likely that IoT growth will continue in this direction. An example is Cisco's plant-watering system. A sensor attached to a bottle of water, poised strategically over a plant, sends information on the plant's water levels to its owner, who may be many miles away. The owner can then decide to reply, indicating to the system that the plant should be watered. The one man-one plant example is remarkable in itself, but has great scope for expansion. Particularly in relatively closed environments like smart cities, such sensors and systems could make maintenance more effective and less time-consuming for humans by taking on tasks like waste management and transportation.

The example of the plant being watered also highlights the other two stages of the IoT system. A 'dumb' sensor will do no more than collect information, but it becomes more useful when connected to an application or process which can analyse this data. This is particularly true as the amount of information collected by various devices in our everyday lives increases. Once the data has been analysed, whatever is relevant can be passed on to the third stage, that of decision making. For more complex decisions, the ultimate decision maker will be a human, who then issues a command (say to water the plant) that makes its way back through the network. Yet it is not inconceivable that for

simpler decisions, the call could be made by a machine. In fact there are currently devices that do just that in the field of agriculture, where there are vehicles which can "drive themselves, inject fertiliser at precise depths, automatically space seeds based on soil fertility and measure harvest data in real time".

While the IoT market will continue to grow and mature globally, India still has a way to go. Reports suggest that despite contributing to the Asia-Pacific statistics mentioned earlier, until 2020 IoT adoption in India will be slow. The Indian government has certainly decided to embrace smart systems, and there are signs that the healthcare, energy and transportation sectors in the country are following suit.

Part of the reluctance to fully support the IoT stems from the risks associated with it. A greater reliance on computerised networks means that if they are not fully secured, they are vulnerable. The consequences of hacking can be significant and widespread. When networks control electricity grids and transportation systems, failures could result in injury to humans and serious setbacks to the economy. This is connected intimately to India's other problem of providing access at affordable prices – somewhere a compromise has to be made. The other issue pertains to the volume of data being collected and stored. Who would have access to this information? Who would control how it would be used? Without a comprehensive privacy protection system in place and in light of concerns about government surveillance (domestic and foreign), people are hesitant to transfer their lives to completely networked systems.

India has taken a proactive step in anticipating the policy questions and regulatory issues that come with a robust Internet of Things network. Its draft policy, though short, covers topics like industry standards, research and development and critically human resource development. Increasing awareness about the Internet of Things, its opportunities and dangers, is essential for the country to succeed. Computers may be getting smarter, but they're still only as smart as the programmers and users behind them.

The author is a Junior Fellow at ORF.

Leave the Internet Alone

Payal Malik & Avirup Bose

More than four decades ago, the Non-Aligned Movement (NAM) launched the concept of a New International Information Order (NIIO).

Its initiative led to the establishment of an independent commission within the fold of the U.N. Educational, Scientific and Cultural Organisation (UNESCO), which produced a report, published in 1980, on a New World Information and Communication Order (NWICO).

The report, titled "One World, Many Voices," is usually referred to as the MacBride Report after its chairman. The very idea of venturing to criticise and challenge the existing global media, namely the information and communication hegemony of the West, touched a raw political nerve, apparently a much more sensitive one than that irked by the developing countries' New International Economic Order (NIEO) proposals.

A determined, no-punches-spared counteroffensive was launched by the Anglo-American tandem, which silenced UNESCO, effectively banning the MacBride Report and excluding the concept of NWICO from the international discourse and U.N. agenda.

The neo-liberal globalisation and neo-con geopolitics tide was on the rise and reigning supreme on the world scene.

The common front of the South was wavering and unsure vis-à-vis the well orchestrated challenge from the North and its multilateral arsenal deployed via the Bretton Woods and WTO troika – and, indeed, via the global media it controlled.

On the defensive and in retreat, with individual countries and their leaders targeted, pressured and tamed, the Global South lowered its profile and, facing stonewalling developed countries, it effectively shelved much of its 1960s/1970s agenda, including its quest for NIIO.

A decade ago, at the World Summit on the Information Society (WSIS), the developing countries did not have the collective will and were not prepared and organised to raise and press these broader issues.

They focused on the "digital divide", as their key concern, which, although important, was not politically sensitive and did not represent a challenge to the existing global information order.

The rise and evolution of the Internet found the South ill-prepared to deal in a comprehensive manner with its implications, challenges and opportunities that it presented, not only for the developing countries individually and collectively, but also for the world order – economic, information and political – and for humankind in general.

The U.N. was marginalised and not allowed in depth to analyse and in an integrated, cross-sectoral and sustained way to deal with the Internet, and as a result did not provide a focus and platform that could have prompted and assisted the Global South in building and evolving its own case and vision.

The Internet-related debates and analyses have largely been focused on and limited to highly specialised and technical, often esoteric, acronym-dominated questions of its governance, which, though of vital importance, has helped to conceal or bypass many fundamental concerns.

Incomprehensible to the general public and not suitable for consideration in multilateral policy forums, the Internet governance deliberations have largely been under control of the world superpower and its cyber mega corporations from Silicon Valley, and the US-centric nature of the Internet has been defended tenaciously and preserved.

The WSIS+10 Review will be taking place shortly. There is an apparent attempt by the West – assisted by its transnational corporations (TNCs) dominating and providing key services on the Internet – to minimise the political importance and limit substantive outputs of this event.

The Group of 77 (G77) and NAM have to focus not only on the non-implementation of the Tunis agenda, but also to work out their position concerning the basic, underlying issues, including the linkages between the Internet and the international development agenda, and, more broadly, the Internet's relevance to the international economic and political order and world peace.

There is the risk that WSIS+10 Review may turn out to be a missed opportunity for the South, and yet another encounter forced to remain within the parameters drawn and preferred by the traditional, well-entrenched masters of the global information and communication order.

Waiting one more decade for the next WSIS+20 Review may not be a recommended approach given the global economic and geo-political trends.

This relative circumspection of the Global South regarding the nature and future of the Internet is compensated in part by the voices coming from some sectors of the civil society that dare stray beyond what is allowed and permissible under the reigning global paradigm.

Thus, for example, the workshop "Organizing an Internet Social Forum", held at the 2015 World Social Forum (WSF) in Tunis, articulated an alternative vision of an Internet and its directions for the future radically different from the current dogma.

And, an international conference on the Internet as a Global Public Resource was recently hosted by government of Malta and DiploFoundation.

"Global public resource" is a term akin to "global public goods". The latter is a concept first launched by the U.N. Development Programme (UNDP) but expurgated from its work and the U.N. discourse during the recent period, probably seen as unsuitable and a threat to the ideological purity of the privatisation gospel, a move to accommodate the political predilections of dominant elites and the current doctrinaire aversion to anything "public".

To move the global debate and multilateral negotiations in a desired direction largely depends on the developing countries as a collectivity, the Global South.

These countries need to grasp the gravity of the systemic issues involved, on par and indeed in some ways more important than those of the traditional international economic, financial, political and social agendas.

The moment is ripe for them to brush up on the original NAM NIIO initiative and the Report of the McBride Commission on NWICO, and consider their relevance in the age of the Internet.

They should work on an alternative vision of the Internet, its functions and governance, which should evolve into the backbone of a future global information and communication order needed in a multipolar world of the 21st century.

Currently, the Internet remains a prisoner of the dominant neo-liberal paradigm and its mantras forced upon the planet by the Western powers and in the service of their global, geopolitical and corporate interests. It needs to be liberated from these shackles. Debate and study that view the Internet from humankind's point of view need to be launched. This will require the Global South to do its homework in depth and fully on the implications and potential roles of the Internet, in order to prepare its platform and press for the initiating of all-inclusive multilateral negotiations and debate.

The BRICS countries together possess the necessary expertise, experience and power to provide the leadership and motor force for mobilising the Global South's collective stand and action on the Internet.

With the high likelihood that the core countries of the West will react negatively, pressure individual

developing countries (as appears to have been the case with Brazil, which has lowered its traditionally forceful public stance on Internet issues), and that obstacles within the U.N. system will persist, doing something concrete independently, via South-South cooperation will be required, and indeed is the only way out of the current impasse.

Here many options exist, including creating supporting institutions and expert bodies and organising regular deliberations, at both technical and political levels.

Bridges should be built with the progressive civil society and possibly with some like-minded countries in the North that are not too happy with the existing system.

The author worked at the U.N. Conference on Trade and Development (UNCTAD), the U.N. Environment Programme (UNEP), the South Commission and was Officer-in-Charge at the South Centre in Geneva (1990-2005).

This article was originally published by the Inter Press Service News Agency, May 21, 2015

Why Smart Cities Need to Get Wise to Security – and Fast

Nicole Kobie

The smart city is an alluring vision of the future, in which civic technology such as traffic lights, smart meters for utilities and public transport could all be connected and feed back invaluable data online.

Glasgow has spent £24m installing technology such as smart street lights that brighten for pedestrians and cyclists, and traffic-tracking sensors in roads, whileBristol is collecting data on everything from health to pollution and interpreting it via a "city operating system". While those cities may be streets ahead of others, most urban areas have some smart features.

Yet a leading internet security researcher has warned that the smart cities of the future could be more vulnerable to hackers than the computers and smartphones of today.

Cesar Cerrudo, chief technology officer at security research firm IOActive Labs, warned that city authorities and governments that are the customers of technology firms aren't testing the security of the systems they buy. "They do a lot of tests for functionality on the system and devices, but they don't do any security testing. So, basically, they are trusting the vendors," he said.

Speaking at the RSA security conference in San Francisco in April, Cerrudo said many firms selling smart systems were failing to build in effective security, such as encryption – a significant problem when so many services transmitted their data wirelessly. "All the data goes over the air. If you don't have a good encryption, anyone can capture the data over the air and compromise security," he said. For example, he revealed that the 200,000 traffic control sensors installed around the world, from Melbourne to London, were vulnerable to attack from hackers.

Sean Sullivan, a security analyst at F-Secure, said: "Smart cities can provide planning departments a lot of very value information for better city living – but it could also be a big vector for fraud unless properly secured.

He agreed that smart cities are "highly hackable" but predicted that we are more likely to see pranks – such as fiddling with highway signs or one-day outages on transport systems that cause chaos – than large-scale attacks.

Sullivan pointed to a smart power meter hack investigated by the FBI that could be costing utility firms millions by letting tech-savvy users reprogramme the meter and get energy for free.

James Lyne, global head of security research at Sophos, said that some systems have relied on security through obscurity.

"To date, the kinds of devices typically deployed to run our critical national infrastructure have relied heavily on obscurity or isolation to keep themselves safe – that is, that they've implemented odd protocols that the mainstream computing world doesn't typically use, and they are placed on isolated networks to try and avoid tampering," said Lyne. "Once one of these principles is degraded, issues are often identified."

Lyne added that: "So far there has not been a concerted effort from the attacker community to compromise such devices. I suspect this is predominantly because it has not met their financial or political goals (the former being the lion's share of attackers' interests).

"The most popular target is still the traditional device used by you or me, as this makes the most money, but of course a more connected future might bring a change in this pattern."

Given the security risks, it may come as a surprise that some internet of things vendors (those who sell appliances and other technology that connects to, and

functions via, the internet) aren't letting researchers such as Cerrudo test their products – even when he's willing to buy them himself.

"Some vendors won't sell it to you if they know you are a security company," he said, without pointing the finger at any specific firms. "That happened to me with a smart street-lighting system. I tried to acquire the devices, but couldn't even get a quote."

Cerrudo said less-established companies saw security research as a threat, despite the practice of more established manufacturers to routinely work with external researchers or hackers to identify security vulnerabilities.

And even when companies did work with security researchers to identify software flaws, it could take months or even years to push out updates to city-wide systems.

"Sometimes they don't have proper mechanisms [for updates], where they can just produce a security fix and get it quickly installed on the systems and devices," he said. "This is a really big challenge, because if they find a security issue, that should be solved very fast. If not, then you remain open to attacks."

What can be done to secure smart cities? Governments need to be more responsible when purchasing smart city solutions, looking not just for whizz-bang features, but taking the time to understand security systems and ensure they actually work.

Cerrudo called for every city to have a Computer Emergency Response Team, or CERT – just as many big businesses do – to handle attacks or vulnerabilities, ensure vendors fix such flaws and run penetration tests to check their own systems.

"In case of a security incident, it will be difficult for a city to know what to do, how to react. A city has plans for earthquakes or floods in some areas, but I don't think many cities have any plans for cyber attacks."

The author is a digital and print journalist specialising in technology writing.

This article originally appeared in The Guardian, May 13, 2015

COMMENTARIES

American Civil Liberties Union, "ACLU Statement Concerning Impending Sunset of Patriot Act Surveillance Authorities", *American Civil Liberties Union Blog*, May 28, 2015

Geoff Grindrod, "Organizational Challenges in the Internet of Things", *Security Intelligence Blog*, May14, 2015

Olaf Kolkman, "Encryption Backdoors Decrease Trust In The Internet", *Internet Society*, May 21, 2015

Devika Agarwal, "Right to be forgotten: A Threat to Freedom of Speech & Expression?",*Spicy IP*, May 15, 2015

Rupam Daniel Frank, "A Neutral Internet", *The Indian Opinion*, May 27, 2015

JOURNAL ARTICLES

Jeanette Hofmann, "Constellations of Trust and Distrust in Internet Governance", in: *Report of the Expert Group 'Risks of Eroding Trust - Foresight on the Medium-Term Implications for European Research and Innovation Policies (TRUSTFORESIGHT)', European Commission, Brussels* http://ssrn.com/abstract=2608414, May 20, 2015

Bhairav Acharya, "The Four Parts of Privacy in India", *Economic and Political Weekly Volume L, No. 22,* May 30, 2015

C Callanan, B Jerman-Blažič, AJ Blažič,"User Awareness and Tolerance of Privacy Abuse on Mobile Internet: an Exploratory Study", *Telematics and Informatics,* Volume 32 Issue 2, May 21, 2015

REPORTS

David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", *United Nations Human Rights Council,* May 2015

Marie Madden and Lee Rainie, "Americans' Attitudes About Privacy, Security and Surveillance", *Pew Research Center*, May 2015

Lennard G. Kruger, "The Future of Internet Governance: Should the U.S. Relinquish Its Authority Over ICANN?", *Congressional Research Service*, May 2015

Office of the Inspector General, "A review of the FBI's use of Section 215 Orders: Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 through 2009", US Department of Justice, May 2015

Iginio Gagliardone and Nanjira Sambuli, "Cyber Security and Cyber Resilience in East Africa", *Global Commission on Internet Governance*, May 2015

Mary Meeker, "Internet Trends 2015 – Code Conference", *Kleiner Perkins Caulfield Byers,* May 2015

BOOKS

Jamie Bartlett, *The Dark Net: Inside the Digital Underworld,* Melville House, May 22, 2015

Charles Murray, *By the People: Rebuilding Liberty Without Permission*, Crown Forum, May 12, 2015

David K. Shipler, *Freedom of Speech: Mightier Than the Sword*, Knopf, May 12, 2015

Anna Bernasek, D.T. Mongan, *All You Can Pay: How Companies Use Our Data to Empty Our Wallets,* Nation Books, May 26, 2015

Ronald Goldfarb, *After Snowden: Privacy, Secrecy, and Security in the Information Age,* St. Martin's Press, May 19, 2015

Opening Speech at the World Summit on the Information Society Forum at Geneva Switzerland

Statement by Mr. Houlin Zhao, Secretary-General, ITU

Geneva Switzerland – May 26, 2015

Your Excellencies, Distinguished Delegates, WSIS Stakeholders, Ladies and Gentlemen,

I should like to express a very warm welcome to all WSIS Stakeholders and representatives from Government, the Private Sector, Civil Society, International Organizations and Academia to the WSIS Forum 2015.

The WSIS Forum continues to grow, going from strength to strength. This year, over 1500 stakeholders are participating in this meeting, including 70 Ministers. More than 120 high level policy statements shall be delivered over the five days of this WSIS Forum 2015.

This growing attendance to the WSIS Forum demonstrates both renewed commitment and dedication by existing stakeholders, as well as growing interest from new partners and stakeholders. So I am delighted to see many familiar faces here today, as well as many new ones. I look forward to learning more about you and your valuable work over this week, and to welcoming you to the WSIS community.

Ladies and Gentlemen,

Over the past ten years, the annual WSIS Forum has become a unique global multistakeholder platform for coordinating and facilitating the implementation of the WSIS Outcomes, in line with the spirit of the original World Summit on the Information Society and Para 109 of the Tunis Agenda.

The WSIS Forum, hosted by ITU and co-organized by ITU, UNESCO, UNDP and UNCTAD, in close collaboration with many other UN Agencies [including WIPO, UNDESA, FAO, UNEP, WHO,, ILO, WMO, UN, ITC, UPU, UNWOMEN, WFP, UNODC and the UN Regional Commissions], has proven an efficient mechanism for coordination of multi-stakeholder implementation activities, information exchange, creation of knowledge, and the sharing of best practices.

The WSIS Forum continues to help stakeholders in developing multi-stakeholder and public/private partnerships to advance development goals and improve people's lives around the world.

2015 is a very special year for ITU and the WSIS process. This year marks the 150th anniversary of ITU that has been working to advance and coordinate telecommunications since it was founded in 1865. 2015 is also a special year for forging links between ICTs, WSIS and Sustainable Development Agenda, taking advantage of the unique opportunity of the two ongoing review processes of WSIS+10 and the Sustainable Development Goals (SDGs).

In this context, the overall theme of the WSIS Forum 2015 is "Innovating Together: Enabling ICTs for Sustainable Development".

We have a very content-rich agenda, with more than 140 sessions building on the official submissions received during the open consultation process. All these Sessions address the tangible work underway and being carried out by governments, private sector, civil society and international organizations.

Later on today, we shall also have the opportunity to recognize their dedication and commitment in the implementation of the WSIS Outcomes by WSIS Prizes honouring and awarding outstanding WSIS stakeholders in the WSIS Prize ceremony 2015.

The WSIS Stocktaking Process continues to give us real stories of on- the-ground implementation and case studies of how ICTs are impacting the lives of people worldwide. You can learn more about some of these from the WSIS Stocktaking Report 2015 that I am now officially releasing. Let me thank for your continuous commitment towards sharing best practices.

Ladies and Gentlemen,

Last year, the highly successful WSIS+10 High-Level Event, and later, the ITU Plenipotentiary Conference 2014 in Busan, Republic of Korea, endorsed two Outcome Documents – namely, the WSIS+10 Statement on the Implementation of WSIS Outcomes and the WSIS+10 Vision for WSIS Beyond 2015. These two Outcome Documents provide fresh vision and renewed priorities for the eleven WSIS Action Lines. They clearly underline the powerful role of ICTs for sustainable development.

The post-2015 process for Sustainable Development has identified ICTs as key enablers of development. However, direct references to the catalytic power of ICTs for development are cited as specific targets only in 4 of the 17 goals (in targets related to education, gender empowerment, universal affordable access to ICTs/internet in LDCs and as a means of implementation). I believe this is not enough, and there should be more targets, to realize the full multiplier effect of ICTs for driving Development.

To underline the key role of ICTs in promoting sustainable development, all WSIS Action Line Facilitators, under coordination by ITU, have developed a WSIS SDG Matrix demonstrating the direct links between the WSIS Action Lines and the SDGs.

Let me use this opportunity to launch officially this live document as initial step towards bringing ICTs on the top of the political agenda. I hope this WSIS-SDG Matrix will serve as an easy reference for all stakeholders engaged in shaping the future of both the SDGs and the WSIS processes beyond 2015, and I encourage you all to use this important tool.

Ladies and Gentlemen,

It is also my pleasure to note that, just after this meeting, the UNGA WSIS overall review process will kick off in New York. We look forward to the outcomes of these deliberations. Let me once again reiterate my support to it this process, making the best possible use of experiences gathered by ITU during the organization of two phases of WSIS (2003-2005) and WSIS+10 High-Level Event, including WSIS+10 Multi-stakeholder Preparatory Platform.

Finally, I would like to thank the partners who have so generously contributed to making this year's WSIS Forum 2015 a success:

- Our Platinum Partner, the United Arab Emirates
- Our two Gold Partners, the Democratic Republic of Congo, and Intel,
- As well as Partners for Specific Activities: Japan, Kuwait, Saudi Arabia and Switzerland.
- Contributing Partners: Poland, Rwanda, ICANN, the Internet Society, and the International Federation for Information Processing.

I wish you all an exciting week ahead. As you know, we won't let you go away empty-handed from the WSIS Forum, and I hope you leave taking with you many fresh ideas, partnerships and collaboration. And we look forward to sharing the Outcomes of the WSIS Forum on the last day of the event.

I wish you all a very successful and productive WSIS Forum 2015.

Thank you.

Source: *International Telecommunication Union*, May 26, 2015

Speech by Günther Oettinger Commissioner for Digital Economy and Society, European Commission, at the 2nd High-level Cyber security Conference,

Brussels, Belgium May 28, 2015

Dear Secretary of State, dear Members of the European Parliament, distinguished representatives from national and regional governments, academia, business leaders, innovators,

Ladies and gentlemen!

It is my honour and my pleasure to welcome you to the second conference on the EU Cybersecurity Strategy.

I would like to thank you all for joining us today.

Introduction – Importance of Cyber security in the Digital Single Market

I am delighted that our event coincides with the beginning of a truly digital era of the European Union. Only three weeks ago Vice-president Ansip and I have presented the Commission's strategy for the European Digital Single Market.

What is at stake when we are talking about the Digital Single Market? 415 billion Euro of additional economic growth to the EU gross domestic product annually, numerous new jobs and a vibrant knowledge-based modern society. We simply have no choice but to provide adequate conditions for the Digital Single Market to flourish.

I am certain that we all agree: there is and will be no efficient and prosperous European Digital Single Market without digital security and trust. European citizens and businesses have to know and trust that the systems underpinning digital services are safe and secure. Therefore, I have made sure that cyber-security – which is the very foundation to trust in online services – is one of the strategy's key pillars and top priorities.

European Strategy on Cyber security

Already back in February 2013, the European Commission and the External Action Service set out a joint vision for "An Open, Safe and Secure Cyberspace". For the first time, the EU took a big step towards safeguarding a secure and open internet for Europe. Its five priorities – increasing cyber resilience; reducing cybercrime; developing our cyber defence policy; fostering EU industry; and promoting our core values internationally – remain essential.

Today, two years after the adoption of this European Strategy on Cybersecurity, in an even more 'digitalised' reality, this conference will review and assess the progress made so far. As with any ambitious strategy, there will be areas where we have delivered, and areas where we still have work to do. And where that is the case, I would urge us all – EU institutions, Member States and stakeholders – to redouble our efforts in order to deliver on our commitments.

Vulnerabilities and cyber attacks

We need to deliver because the digital world is becoming more and more vulnerable. As much as great inventions and technologies empower us, their failure – or their conscious misuse – can also lead to unprecedented damage and pose real threats.

Technical failures and malicious attacks occur at alarming and ever increasing intervals. Inadequate response to these incidents result in consumers losing confidence, businesses losing money and even national security being put at stake.

Statistics are truly alarming. Each minute somewhere around the world a cyber-attack is being performed.

Now, literally this very second, someone's computer is being hacked, someone's personal records, financial information, or intellectual property is being stolen and sold on the black market. Someone is losing money as a result of that attack. This 'someone' could be me, you, or your bank, university or government.

Let us not forget: criminals are stepping up their game and data breaches are increasingly common and devastating. That is why we need to act together.

Cyber breaches happen for multiple reasons. Whatever the motivation and whoever the attacker -- they are all far too common and their consequences are far too costly. Over 75 % of small businesses and 93% of large ones have suffered a cyber-attack. Costs can run into the millions, not to mention the catastrophic market loss and reputational damage.

The number and impact of cyber incidents continue to grow. We have to cooperate better and more efficiently than ever before. It is evident: vulnerabilities, backdoors and incidents need to be detected and acted upon as early as possible. Many companies suffer cyber-attacks without knowing that they are being victims of it.

That is why I consider cross-border, European co-operation essential. Let us not forget that what can happen in one Member State could also happen in another. And while there are some Member States who may be better equipped than others, no Member State is immune. Together we are stronger.

The latest revelations about the attack on TV5 prove that our powers are limited in the face of digital assaults by militant groups. Only five years ago it would have been difficult to imagine that hackers would take control of a prominent TV channel and cut off broadcasting for a day.

This attack against TV5 Monde, well prepared for weeks, signals a new level of threat to Western media – but it is a clear warning signal as well for other civilian and military networks.

Our critical infrastructures are also vulnerable. For example, the port of Antwerp was hit by cyber-attacks over a two-year period from June 2011.

The attackers infiltrated computer networks in at least two companies operating in the port of Antwerp, thereby enabling a trafficking group to hide cocaine and heroin among legitimate cargoes.

The breach allowed hackers to access secure data giving them the location and security details of containers, meaning the traffickers could send in lorry drivers to steal the cargo before the legitimate owner arrived.

In other circumstances, our citizens are also at risk. Just a couple of weeks ago, the press reported that visitors to the website one of UK's most famous chefs, instead of finding recipes, were actually served malware.

European response to Cybersecurity

So how do we strengthen cybersecurity in Europe? I have three priorities:

1)Bringing cybersecurity capabilities and cooperation to maturity

2)Making the EU a leader in cybersecurity

3)Mainstreaming cybersecurity in EU policies

1) Let me come to my first priority – it is about bringing cybersecurity capabilities and cooperation to maturity.

The foundation of our approach is the proposed Directive on Network and Information Security. We are in the final stages of the negotiations and I call on the Member States and the European Parliament to reach a meaningful agreement very soon. It has taken already too long and we have a duty to our citizens to act.

We need a high common level of cybersecurity across the EU.

First, we need improve member states cybersecurity capabilities that are now uneven across the EU. This means setting up the necessary national structures – particularly Computer Emergency Response Teams. The EU of course already has one in place for its own institutions.

Second, we need to enhance cooperation between the Member States, which now takes place in small and closed circles.

And third, we need to ensure a high level of risk management practices, so that our critical infrastructure has the right security measures in place to get as immune as possible against cyber-attacks. Both public and private infrastructure is concerned. And both traditional infrastructure, such as energy and transport; and modern – such as the internet platforms which all of us, and the digital economy, rely on every day.

I agree – these solutions will be resource-intensive; they may and probably will imply necessity for reorganization, revision of practices and processes within concerned institutions and businesses. But we have no choice. The price for vulnerabilities and technical failures would be much higher.

Moreover our businesses, economy and even society will be weaker if the Directive has insufficient impact on our trusted and secure networks. We need an ambitious text – and the Commission is ready to work to that aim.

An ambitious Directive will create an enabling framework, but this is only the starting point: we also need determination, creativity and a proactive approach to make sure that visible progress will come. This is particularly true for cooperation, it has to be *meaningful*. So we need not only to coordinate our policies but also to actually work together on real-life cyber incidents. And we need to do further work to apply the principles of risk management to the specific sectors of the economy.

I'd like to thank the Latvian Presidency and the European Parliament for their work and restless efforts to reach a political agreement on the Directive. I fully support the aim of a swift deal on an ambitious text as we have no more time to waste.

2) The second priority is making the EU a leader in cybersecurity.

Unlike other areas of the digitalised world, the European cybersecurity industry is still, in many areas, leading: we have, in the European Union, companies that are best in class in providing trusted technologies.

However, we lag behind in many areas of ICT. And this is worrying, since this threatens also the very positive position the European cybersecurity industry has.

Keeping or even enhancing the industry's frontrunner position in the area of cybersecurity means fostering trustworthy European solutions for protecting citizens, companies and public institutions on line, in a global market expected to grow to between $80 and $120 billion by 2017.

And this also means that Europe needs to be more ambitious in cybersecurity. Both in the public sector and in the private sector.

We must nurture the competitive advantage of our cybersecurity industry, the skills and investments that they rely upon. If the issue of technological sovereignty has been raised in past few years it is not because of a desire to shy away and become protectionist from a globally competitive market.

The debate about technological sovereignty has arisen out of a realisation that freedoms and values that we cherish in Europe are at risk. There are some who do not respect privacy of our citizens. Some do not want to play on fair terms with our businesses. We need to safeguard our values and interests.

It is in the interest of all citizens that we ensure a prosperous and a secure European digital future. That means that we have to be leaders in these technologies and support international standardisation efforts that ensure high levels of security, proven by certification where necessary. Such an approach will benefit everyone in the digital world that shares our values and wants to safeguard them in a future digital economy that is truly global. The value of our digital economy stems precisely from the fact that it is global, and open and, I would add, trustworthy.

The Digital Single Market strategy announced that the Commission will propose a public-private cooperation for research and innovation in 2016. I very much hope that it will ensure easy and affordable access to the latest digital security technologies, secured infrastructures and best practices.

It will build on the extensive research and innovation support provided in the past by the Framework Programme 7 and in Horizon 2020 now totalling more than 500 Million Euro between 2014 and 2020. Our experiences show that there is scientific excellence and momentum among European researchers and entrepreneurs – we want to help them to make breakthrough on the global marketplace.

The NIS Platform also plays a very important role. Many of you here are active members and participants. The aim of the Platform is to identify good cybersecurity practices that are applicable to the whole ICT value chain and in particular to SMEs. It is providing valuable input into future research and innovation in cybersecurity, privacy and trust. It proposes new ways to promote truly multidisciplinary research. The Platform met for its 5th Plenary yesterday (27 May) and finalised guidance documents on cybersecurity risk management approaches and voluntary information-sharing. It will also shortly publish the final version of its Cybersecurity Strategic Research Agenda.

3) And finally the third priority is mainstreaming cybersecurity in EU policies.

This means making sure that cybersecurity is taken into account throughout the policy-making process. Particularly when we think about new technologies and emerging sectors - like smart cities, connected cars, smart grids or eHealth, the internet of things or Industry 4.0 – to name just a few. We all need to "think cyber security" right from the start, so that risk management and other key elements are addressed properly and effectively in all aspects of the policy. This is the best way to ensure that cybersecurity is embedded in our future policy initiatives and not just an after-thought – which as we all know cannot provide an adequate solution.

Conclusions

Ladies and gentlemen, as I said at the beginning, cybersecurity is a shared European mission – or has to become one, where this is not yet the case. Against that background I am sure that the three priorities that I have set out can together provide the strong foundations in trust and security that are needed in order to make the Digital Single Market a reality.

Thank you.

Source: *European Commission*, June 1, 2015