CYFY
THE INDIA CONFERENCE ON CYBER SECURITY AND CYBER GOVERNANCE

OBSERVER RESEARCH FOUNDATION

ORF CYBER MONITOR

CYFY 2015 14th to 16th October

VOLUME III | ISSUE 1 | JANUARY 2015 | http://cyfy.org

COMMENTARY

Net Neutrality and the Law of Common Carriage

Bhairav Acharya

Net neutrality makes strange bedfellows. It links the truck operators that dominate India's highways, such as those that carry vegetables from rural markets to cities, and Internet service providers which perform a more technologically advanced task.

Drones are welcome, but where's the policy framework?

R Swaminathan

The Delhi police proposal to use drones for day-to-day law and order activities is bound to fail unless it is accompanied by a regulatory and manufacturing ecosystem for unmanned aerial vehicles

Book Review: The Electronic Silk Road

Mahima Kaul

The argument for an electronic silk road, promoting free trade and by extension, harmonious global values and laws, is an inherently appealing idea to all digital natives used to an 'open web experience'.

When is Personal Info Fair Game?

Anahita Mathai

In November 2014, Sony Pictures Entertainment was hacked. Given the nature of the stolen information, decisions about publishing it were made decidedly more complicated than usual.

The future of the internet is up in the air

Alex Pearlman

The internet as you know it is about to fundamentally shift. Big changes are ahead, and there's been a surprising lack of discussion about how the web we've come to know and love will be managed, and who will be at the helm.

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

ESSENTIAL READINGS

STATEMENTS

Turn to Page # 21

EDITORIAL

Editors

Governance

The year 2014 was hugely significant for internet governance, as the 25th anniversary of the development of the World Wide Web was celebrated globally. The first month of 2014 saw the establishment of the Global Commission on Internet Governance (GCIG), launched by the Centre for International Governance Innovation and Chatham House. The GCIG, envisioned as a two-year project, seeks to "articulate and advance a strategic vision for the future of Internet governance." The Commission is headed by former Swedish Prime Minister Carl Bildt and emerged in the light of 'growing state control of online activities'.

Continuing fallout from the Snowden revelations produced some radical ideas, including a proposal by German Chancellor Angela Merkel to build a communications network for Europe alone. The efforts to improve data protection in Europe were echoed by the French government. The two governments said the network would help alleviate concerns about surveillance being conducted as data travelled around the world.

In response to global concerns that it was controlling too much of the internet's infrastructure, the United States announced that it was giving up control of the Internet Corporation for Assigned Names and Numbers (ICANN), which operates key functions of the internet. The move was widely seen as opening the door for a multistakeholder model of governance to emerge.

2014 was also a big year for conferences. The first was NETmundial, the Global Multistakeholder Meeting on The Future of Internet Governance, held in Brazil. Involving participants from all around the world at various levels of governance, the conference's focus was on "the elaboration of principles of Internet governance and the proposal for a roadmap for future development of this ecosystem". The meeting produced an outcome statement, which was criticised by some for its non-binding nature and what was perceived to be a watering-down of some key issues like mass surveillance and net neutrality.

In June 2014, the 50th meeting of ICANN was held in London. One of three yearly meetings, the London session of ICANN featured discussions on the globalisation of the Internet Assigned Numbers Authority (IANA) and the release of a report by the Expert Working Group (EWG) on issues of privacy and more.

The Plenipotentiary Conference of the International Telecommunications Union (ITU) took place in South Korea from October to November. Several controversial proposals had been made prior to the start of the conference, on issues including server hosting, IP address allocation, the role of governments and online privacy. However in the end, possibly as a result of backchannel meetings between delegations, these proposals were diverted to the Working Group on the internet.

In September, Turkey hosted the ninth edition of the Internet Governance Forum (IGF), which caused some consternation given Turkey's record with internet rights. In some ways the future was hanging in the balance, since the future of the IGF will be decided by the UN in December of this year. More than 2000 people attended the conference, hailed as the best place to get a sense of the wide scale of the internet governance landscape. Topics discussed included net neutrality, data localisation and human rights.

The second edition of Cyfy, the India Conference on Cyber Security and Cyber Governance was held from October 15-17. Organised by the Observer Research Foundation, the conference saw participation from more than a dozen countries speaking in 14 sessions.

A ruling in May by the Court of Justice of the European Union upheld the 'right to be forgotten', requiring Google to remove links to "inadequate, irrelevant or no longer relevant, or excessive" information about individuals. By the end of the year, the right to be forgotten had expanded beyond the European versions of Google to include Yahoo and Bing . There have also been calls for the removal of links to internationally, to all versions of Google.

European concerns about privacy and surveillance are being addressed by legislators, and the European Union is well on its way to achieving a comprehensive privacy framework through the EU General Data Protection Regulation.

The number of government requests for user data that are received and complied with by large corporations like Google and Facebook are increasing. One positive step was that in the USA, an agreement was reached which permitted companies to reveal how many information requests they were receiving from national security agencies.

Issues of cyber jurisdiction came to the fore with a mid-year ruling against Microsoft. An American court held that a search warrant issued in the US for data stored on servers in Ireland was valid. The case is yet to be resolved, but the Irish government is now involved, taking a stance over their sovereignty in the cloud.

Artificial intelligence (AI) has been making strides, which has caused some to worry. One of the most prominent figures voicing concern was physicist Stephen Hawking, who went so far as to say AI could 'end mankind'. Mathematicians, philosophers, writers and businessmen also joined Hawking in warning that the development of AI could lead to complex issues which were not being given due consideration.

Though not yet sentient, devices are becoming ever more interconnected. The phenomenon, the Internet of Things (IoT) imagines a scenario whereby everything electronic is connected through a central hub - like a smartphone. While the idea has been embraced by many as a concept, others have noted that there is much work to be done to successfully integrate the technologies.

The newly-elected government in India, led by Narendra Modi, approved and launched the "Digital India" programme to "transform India into a digital empowered society and knowledge economy". The ambitious project seeks to expand India's National Optical Fibre Network and the National Broadband Mission to connect everyone in India to the internet and provide e-governance services.

Several companies announced drone-based initiatives to increase wi-fi connectivity. The need for legislation to deal with the commercial and recreational use of drones was also a topic that picked up steam in 2014. Several aviation regulatory boards around the world initiated or expanded plans to deal with the issue.

Late in the year, police forces in Sweden raided several locations and confiscated severs and other hardware related to file-sharing site The Pirate Bay (TPB), leading to the site going offline. Copyright holders had long been seeking to shut down TPB, but the site became notoriously resilient and was a byword for pirated content.

Security

Cyber security was one of the defining aspects of 2014 with cyber hacks and cyber warfare gaining spotlight in world politics. Most high profile cyber security hack occurred in December 2014 when Sony Pictures was hacked by a group called "Guardians of Peace" leading to several unreleased movies being leaked on the internet. The violation occurred in response to Sony Picture's planned release of the film 'the Interview'; a satire centred on a plot to assassinate the North Korean leader Kim Jong-un. Several US agencies accused North Korea of orchestrating the hack which led to massive financial losses for Sony Pictures. Furthermore, Sony Picture was threatened with additional consequences if it went ahead with its planned release of the Interview. Despite reassurances from the US government, several prominent theatre chains refused to screen the movie leading to Sony Pictures cancelling the release. President Obama strongly criticised Sony's decision to cancel the release stating foreign actors could not be allowed to dictate

US domestic culture. After global outcry against cancellation of the release, Sony Pictures eventually decided to release the film online prompting further threats from the North Korean regime. Interestingly, reports emerged of widespread internet outages in North Korea a few days after President Obama's statement. Cyber experts claimed such outages were consistent with cyber attacks.

There were some other major breaches in 2014 as well. The infamous celebrity cloud leak, which led to collections of intimate celebrity images leaked online. Since then Apple has staunchly denied any vulnerabilities with its iCloud, although some of the released files were confirmed to have been housed in iCloud. Similarly, a list of almost five million Gmail addresses and passwords hacked from various websites was posted on a Russian online forum. Google said the leak was one of several so-called credential dumps that the company spotted. It also emerged that Cyber criminals were using a new malware -- Regin -- to penetrate and monitor GSM networks in India and other countries including Pakistan, Brazil, Germany and Russia. An elaborate, three-year cyber-espionage campaign against United States military contractors, members of Congress, diplomats, lobbyists and Washington based journalists was linked to hackers in Iran. The campaign compromised the computers of some 2,000 victims and went unnoticed since 2011. In what was termed as the biggest international hacking scandal, possibly involving corporate, associations and big individuals, coordinated raids were conducted by investigative agencies in India, China and Romania, on the basis of intelligence from Federal Bureau of Investigation about the "organised hacking" happening in three countries and others. JP Morgan Chase, one of the largest banks in the US, admitted that a massive computer hack affected the accounts of 76 million households and about seven million small businesses, making it one of the largest of its kind ever discovered.

Due to the spike in cyber attacks, governments around the world took to creating additional measures aimed at securing and preventing such attacks. The Pentagon is planning to more than triple its cyber security staff in the next few years, Defence Secretary Chuck Hagel had said. Russia and China are all set to sign an international cyber security agreement in the first half of 2015. The document was initially planned to be approved during President Vladimir Putin's visit to China. However, it was decided that the agreement should be made "more extensive and practical" and that this would take several more months. Furthermore, by 2017, the Russian Defense Ministry is planning to complete the formation of a special cyber security force designed to protect the army from computer attacks. The move is part of a federal program to modernize the country's information security. Amid concerns of Iran's increasingly enhanced ability to wage cyber warfare, Prime Minister Binyamin Netanyahu announced the upgrading of Israel's cyber defense with the establishment of a new National Cyber Defense Authority that will protect civilian cyberspace, and not just vital security facilities. President Abdel Fattah Al-Sisi approved the adherence of Egypt to an Arab convention that will see greater cooperation within the Arab states on matters of cyber security. The president's decree saw Egypt sign the Arab Convention for Combating Information Technology Crimes.

In the world of business, Boeing plans to open a cybersecurity analytics facility in Singapore, its first outside the United States, as part of efforts to make such capabilities and services accessible to customers in the Asia-Pacific region. The new facility will hire and train cybersecurity professionals locally, carry out advanced analytics, and support the aviation company's regional cybersecurity center of excellence. KPMG completed the acquisition of P3, a privately-owned German cyber-security firm that provides risk management, security assessments, and mobile and fixed network protection to clients across the financial services sector. SingTel will invest S$500 million ($395 million) over the next five years and hire 1,000 engineers as part of a three-pronged strategy to build strengths in cyber security, smart cities and analytics. Microsoft acquired Aorato Ltd., an Israel-based cybersecurity startup for 200 million. General Motors Co. named an engineer to serve as its first Cybersecurity Chief as the No. 1 U.S. automaker and its rivals come under increasing pressure to better secure their vehicles against hackers. The Food and Drug Administration in United States is asking the public to weigh in on the cybersecurity of medical devices and holding a conference on the subject, organized in

collaboration with the Department of Homeland Security. Raytheon announced its acquisition of privately held Blackbird Technologies, which provides cyber security, surveillance and secure communications to spy agencies and special operations units, for $420 million. While Spanish cybersecurity firm S2 Grupo confirmed that it will begin operating in Colombia in the first quarter of 2015 as part of an expansion effort that also includes plans to set up shop elsewhere in Latin America and other parts of Europe later this decade.

Net Neutrality and the Law of Common Carriage

Bhairav Acharya

Net neutrality makes strange bedfellows. It links the truck operators that dominate India's highways, such as those that carry vegetables from rural markets to cities, and Internet service providers which perform a more technologically advanced task. Over the last decade, the truckers have opposed the government's attempts to impose the obligations of common carriage on them, this has resulted in strikes and temporary price rises; and, in the years ahead, there is likely to be a similar – yet, technologically very different – debate as net neutrality advocates call for an adapted version of common carriage to bind Internet services.

Net neutrality demands a rigorous examination that is not attempted by this short note which, constrained by space, will only briefly trace the law and policy of net neutrality in the US and attempt a brief comparison with the principles of common carriage in India. Net neutrality defies definition. Very simply, the principle demands that Internet users have equal access to all content and applications on the Internet. This can only be achieved if Internet service providers:(i) do not block lawful content; (ii) do not throttle – deliberately slow down or speed up access to selected content; (iii) do not prioritise certain content over others for monetary gain; and, (iv) are transparent in their management of the networks by which data flows.

Almost exactly a year ago, the District of Columbia Circuit Court of Appeals – a senior court below the US Supreme Court – struck down portions of the 'Open Internet Order' that was issued by the Federal Communications Commission (FCC) in 2010. Although sound in law, the Court's verdict impeded net neutrality to raise crucial questions regarding common carriage, free speech, competition, and others. More recently, Airtel's announcement of its decision to charge certain end-users for VoIP services – subsequently suspended pending a policy decision from the Telecom Regulatory Authority of India (TRAI) – has fuelled the net neutrality debate in India.

Because of its innovative technological history in relation to the Internet, the US has pioneered many legal attempts to regulate the Internet in respect of net neutrality. In 1980, when Internet data flowed through telephone lines, the FCC issued the 'Computer II' regime which distinguished basic services from enhanced services. The difference between the two turned on the nature of the transmission. Regular telephone calls involved a pure transmission of data and were hence classified as basic services. On the other hand, access to the Internet required the processing of user data through computers; these were classified as enhanced services. Importantly, because of their essential nature, the Computer II rules bound basic services providers to the obligations of common carriage whereas enhanced services providers were not.

What is common carriage? Common law countries share a unique heritage in respect of their law governing the transport of goods and people. Those that perform such transport are called carriers. The law makes a distinction between common carriers and other carriers. A carrier becomes a common carrier when it "holds itself out" to the public as willing to transport people or goods for compensation. The act of holding out is simply a public communication of an offer to transport, it may be fulfilled even by an advertisement. The four defining elements of a common carrier are (i) a holding out of a willingness (a public undertaking) (ii) to transport persons or property (iii) from place to place (iv) for compensation.

Common carriers discharge a public trust. By virtue of their unique position and essential function, they are required to serve their customers equally and without discrimination. The law of carriage of goods and people places four broad duties upon common carriers. Firstly, common carriers are bound to carry everyone's goods

or all people and cannot refuse such carriage unless certain strict conditions are met. Secondly, common carriers must perform their carriage safely without deviating from accepted routes unless in exceptional circumstances. Thirdly, common carriers must obey the timeliness of their schedules, they must be on time. And, lastly, common carriers must assume liabilities for the loss or damages of goods, or death or injuries to people, during carriage.

The Computer II regime was issued under a telecommunications law of 1934 which retained the classical markers and duties of common carriers. The law extended the principles of common carriage to telephone services providers. In 1980, when the regime was introduced, the FCC did not invest Internet services with the same degree of essence and public trust; hence, enhanced services escaped strict regulation. However, the FCC did require that basic services and enhanced services be offered through separate entities, and that basic services providers that operated the 'last-mile' wired transmission infrastructure to users offer these facilities to enhanced services providers on a common carrier basis.

In 1996, the new Telecommunications Act revisited US law after more than sixty years. The new dispensation maintained the broad structure of the Computer II regime: it recognised telecommunications carriers in place of basic services providers, and information-services providers in place of enhanced services. Carriers in the industry had already converged telephone and Internet communications as a single service. Hence, when a user engaged a carrier that provided telephone and broadband Internet services, the classification of the carrier would depend on the service being accessed. When a carrier provided broadband Internet access, it was an information-services provider (not a telecommunications carrier) and vice versa. Again, telecommunications carriers were subjected to stricter regulations and liability resembling common carriage.

In 1998, the provision of broadband Internet over wired telephone lines through DSL technologies was determined to be a pure transmission and hence a telecommunications service warranting common carriage regulation. However, in 2002, the FCC issued the 'Cable Broadband Order' that treated the provision of cable broadband through last-mile wired telephone transmission networks as a single and integrated information service. This exempted most cable broadband from the duties of common carriage. This policy was challenged in the US Supreme Court in 2005 in the *Brand X* case and upheld.

Significantly, the decision in the *Brand X* case was not made on technological merits. The case arose when a small ISP that had hitherto used regular telephone lines to transmit data wanted equal access to the coaxial cables of the broadcasting majors on the basis of common carriage. Instead of making a finding on the status of cable broadband providers based on the four elements of common carriage, the Court employed an administrative law principle of deferring to the decisions of an expert technical regulator – known as the Chevron deference principle – to rule against the small ISP. Thereafter wireless and mobile broadband were also declared to be information services and saved from the application of common carriage law.

Taking advantage of this exemption from common carriage which released broadband providers from the duty of equal access and anti-discrimination, Comcast began from 2007 to degrade P2P data flows to its users. This throttling was reported to the FCC which responded with the 2008 'Comcast Order' to demand equal and transparent transmission from Comcast. Instead, Comcast took the FCC to court. In 2010, the Comcast Order was struck down by the DC Circuit Court of Appeals. And, again, the decision in the *Comcast* case was made on an administrative law principle, not on technological merits.

In the *Comcast* case, the Court said that as long as the FCC treated broadband Internet access as an information service it could not enforce an anti-discrimination order against Comcast. This is because the duty of anti-discrimination attached only to common carriers which the FCC applied to telecommunications carriers. Following the *Comcast* case, the FCC began to consider reclassifying broadband Internet providers as telecommunications carriers.

However, in the 2010 'Open Internet Order', the FCC attempted a different regulatory approach. Instead of a classification based on common carriage, the new rules recognised two types of Internet service providers: (i) fixed providers, which transmitted to homes, and, (ii) mobile providers, which were accessed by smartphones. The rules required both types of providers to ensure transparency in network management, disallowed blocking of lawful content, and re-imposed the anti-discrimination requirement to forbid prioritised access or throttling of certain content.

Before they were even brought into effect, Verizon challenged the Open Internet Order in the same court that delivered the *Comcast* judgement. The decision of the Court is pending. Meanwhile, in India, Airtel's rollback of its announcement to charge its pre-paid mobile phone users more for VoIP services raises very similar questions. Like the common law world, India already extends the principles of common carriage to telecommunications. Indian jurisprudence also sustains the distinction between common carriage and private carriage, and applies an anti-discrimination requirement to telecommunications providers through a licensing regime.

TRAI must decide if it wants to continue this distinction. No doubt, the provision of communications services through telephone and the Internet serves an eminent public good. It was on this basis that President Obama called on the FCC to reclassify broadband Internet providers as common carriers. Telecommunications carriers, such as Airtel, might argue that they have expended large sums of money on network infrastructure that is undermined by the use of high-bandwidth free VoIP applications, and that the law of common carriage must recognise this fact. And still others call for a new approach to net neutrality outside the dichotomy of common and private carriage. Whatever the solution, it must be reached by widespread engagement and participation, for Internet access – as the government's Digital India project is aware – serves public interest.

The author is a constitutional lawyer and advises the Centre for Internet and Society (CIS), India, on legal issues.

Drones are welcome, but where's the policy framework?

R Swaminathan

The recent rape of a young woman in an Uber taxi in Delhi has triggered off a slew of institutional responses. These range from usual suspects like increased patrolling by the police to the unusual ones like the use of drones to keep an eye on activities. It's interesting that the Delhi police are actively looking at deploying drones to augment and, in several cases, take over standard policing operations. At one level, it's almost an explicit admission that their existing system of patrolling and response mechanisms – the basic framework of law and order – are fraying at the edges, often getting overwhelmed comprehensively by the ugly underbelly of the city. At another, it indicates a desperate and naïve assumption that just throwing high end technology at a deep rooted and multidimensional problem, one that's as social and economic and it is gendered and political, will end up resolving it. By itself technology cannot be the sole solution to social issues. However, a robust ecosystem of technology-based solutions combined with the right administrative structure and a proactive policy environment can actually contribute to a better quality of life and a safer and more secure cityscape. A good example is the staggered manner in which New York mayor Michael Bloomberg set the stage for introducing drones for internal surveillance and law and order functions. Of course, it wasn't without its share of controversies, especially on issues of privacy, but the public debate it generated contributed a great deal in clarifying the operating profile and the policy framework for the use of drones on a daily basis. Seen in this context, the decision of the Delhi police to use drones seems like an ad-hoc and knee-jerk reaction with no clear-cut thought process on how it will integrate with the existing systems of investigation, evidence gathering and recording and standard operating procedures. In order for drones to effectively augment existing police functions and create new ways of responsive intervention and action, instead of becoming yet another fancy and underutilised toy, there is a clear cut need for an enabling system. There are three fundamental pillars for creating this facilitating framework.

The first is to clearly reorient and redefine notions of airspace and air-corridors. A drone is an unmanned aerial vehicle first and an integrated digital system next. Indian policy makers tend to treat airspace as somewhat of a physical commodity, almost like a piece of land. It's necessary to look at airspace beyond its literal definition and as a 'collection of procedures, regulations, infrastructure, aircraft and personnel that compose the national air transportation system'. Airspace, by default, has also come to mean at least 10,000 feet. Except for the landing and take-off phase, for airlines, air traffic controllers, aviation authorities and policymakers airspace only refers to 25,000 to 35,000 feet (the standard cruising altitude for most civilian aircraft). Micro drones and small unmanned aerial vehicles, like the ones being sought to be used by Delhi police, redefine airspace with some cruising at less than 100 feet and others going up to almost 3000 feet. Though not many details are available, the drones expected to be used by the Delhi police will have the capability to transmit real time pictures to Quick Response Teams (QRTs), integrate with the existing network of CCTV cameras and fly at approximately 200 feet. The prevailing Air Traffic Control (ATC) system operates on the basis of ground level radars (a command centre) monitoring the movement of planes, and communicating directly with the pilots and co-pilots on direction, altitude, navigation, vehicle and traffic control and collision avoidance. Apart from the constant guidance and inputs from the ATC, pilots either visually try and spot aerial vehicle or use the Traffic Collision and Avoidance System (TCAS) to avoid untoward incidents. Unmanned aerial vehicles have to integrate with the current system, especially with the TCAS. This requires the current ATC system to introduce new generation radars that can track small and microdrones flying at extremely low altitudes. Additionally a system to physically and electronically

identify drones has to be evolved. Since drones will increasingly become part of a networked environment, it's critical to give each drone a unique electronic code, something like an Internet protocol address, for quick, easy and clear identification. In this regard, the European Union's policy and approach document towards the regulation and management of unmanned aerial vehicles is an excellent starting point.

The second is to reconceptualise connectivity and infrastructure. Drones are, for all practical purposes, the first autonomous peer-to-peer connective infrastructure that does not need a hub. Though each drone is an independent hub and a spoke at a same time, nonetheless they require adequate docking and charging stations. If the Delhi police is serious about integrating drones as part of its law and order maintenance and surveillance system then it has to first establish specifically earmarked docking and recharging stations. Most of these drones are either electrically and battery operated or work on alternative energy means like solar energy. The docking and maintenance stations will require their own power sources, an entire band of unmanned aerial vehicle engineers, maintenance crew and a complete supply chain system for parts, electronics and networking solutions. There is also a need to support and evolve a domestic drone industry that understands specific Indian challenges. Today, most of the drones are imported and then customised. These two aspects, of a evolving a docking and maintenance infrastructure and a robust domestic industry, cannot be achieved till all aspects of civilian drone management and regulation is integrated into one single department. The issues of integration of unmanned aerial vehicle with existing systems of law and order transcend boundaries of civil aviation, internal security, privacy and safety and external security. A crucial component of resolving this challenge to satisfaction is to reorient the role of DGCA from an agency focusing exclusively on providing various forms of certifications for flight operations, air worthiness and the final Certificate of Authorisation (COA), and to become a true regulator on the lines of a Securities Exchange and Board of India (SEBI) and Telecom Regulatory Authority of India (TRAI). In this respect it would be a good idea to look at the policy measures being taken in the United States of America to expand the regulatory mandate of the FAA to slowly integrate drones with the existing manned aviation network. Today, FAA has a separate division that's exclusively mandated to look and manage the integration of drones into various daily aspects of social, political and economic life.

The third issue is one of privacy. Taken together with CCTVs, web monitoring programmes and real time satellite imagery, drones complete the picture of 360 degree surveillance. Drones require an absolutely new human thinking: one that has to acknowledge and understand that the set of interconnected technologies of today constitute an artificial intelligence of tomorrow that will no longer be completely in our control. It is in this context that there are two fundamental challenges that are worth considering and debating. The first challenge confronting Indian policy makers is to substantially rework the Information Technology Act of 2000, which was amended in 2008, to be ready for a future that's going to be increasingly based on an Internet of things. Drones are at the cutting edge of this phenomenon. Attention has to be paid to Section 66A of the IT Act, especially its wordings **'computer resource'** and '**communication device',** which embeds the possibility of any land or air vehicle, whether manned, semi-autonomous and completely autonomous, using any form of digital technology, which for all practical purposes is a computer resource, to come within the purview of the Information Technology Act. The second challenge is to redefine existing legal framework with reference to what constitutes the correct way of collecting evidence, especially its admissibility in a court of law in the context of Indian attempts to define a comprehensive and proactive policy and regulatory framework for privacy. The Information Technology (Amendment) Act, 2008 has two sections -- 43A and 72A -- providing for civil and criminal liabilities relating to Privacy. Section 43A focuses on the nuts and bolts of 'reasonable security practices' for sensitive personal data and information, while Section 72A provides for a jail term and a fine to anyone, a person, a body corporate or an institution, who causes 'wrongful loss or wrongful gain' by divulging the personal information of another person. These two sections specifically defined personal data as any information that is capable of singularly identifying the person. Everything from birth registry details, hospital records, financial

and census information, mobile number, social networking details, educational records to death certificate and even a person's sexual orientation can possibly be interpreted to mean personal data and information. The introduction of drones for law and order introduces a completely new dimension to the debate and it's within this context that the draft Privacy Bill 2011 needs to be located. In this context, it would also not be a bad idea examine the case history relevant to drone surveillance and the American Fourth Amendment, especially how the Katz vs United States (1967) case, which established a legal and juridical standard for the interpretation of the Fourth Amendment, has been used in recent times to redraw and reorient 'constitutional protections' of the United States of America.

The author is a Senior Fellow with the Observer Research Foundation, a Fellow of the National Internet Exchange of India (NIXI) and Contributing Editor of Governance Now

Book Review – "The Electronic Silk Road: How the Web Binds the World Together in Commerce"

Mahima Kaul

The argument for an electronic silk road, promoting free trade and by extension, harmonious global values and laws, is an inherently appealing idea to all digital natives used to an 'open web' experience. Dr Anupam Chander, himself a product of parents who migrated from India to the US in search of a better life, expertly lays bare the changes in global trade patterns – and the resulting complications – in his book 'The Electronic Silk Road: How the Web Binds the World Together in Commerce,' released in 2014 in South Asia. Aside from the easy narrative exploring complicated developments, Chander's book is especially pertinent for an Indian audience, looking to profit off this free trade, often without reading the fine print.

The promise of Trade 2.0 is enormous, begins Chander, but he quickly delves into the real world complications that arise out of these new exchanges. Unlike with goods trade, where a well-defined port of entry and exit serves as points for regulation and new jurisdictions, digital exchanges of services, prove to be far trickier. He raises a metaphysical question: where does an event in cyberspace occur? Simply put, whose jurisdiction extends to these digital transactions – the region where the company providing the services is registered, or the region where these services are consumed?

The real-life examples of the 'pirates of cyberspace' are easier understood. For example, the gambling sites operating out of Antigua, where it is legal, were sorely contested in the USA, where, for the most part gambling is illegal. This particular case went to the WTO where the gambling sites argued that they were simply providing entertainment services while the US argued that this sort of activity would promote fraud, money laundering and underage gambling. The WTO sided with the US. Another case, familiar to most young people, is of the file-sharing site, The Pirate Bay, which is under constant legal threat from copyright holders because of the "illegal" downloading of materials that include movies and music. The founders have even been convicted of copyright infringement under Swedish law, and have since moved their domain name from .org to the Swedish address .se to avoid the risk of seizure of their domain name by the US authorities.

This move too, speaks to the parallel jurisdictions that exist in cyberspace, complicating its 'free flow.' In fact, the domain name system is described by Chander as 'choke point' in an essentially end-to-end system. What this means is that the body that sets rule for domain names, Internet Corporation for Assigned Names and Numbers, ICANN, can function as an otherwise elusive chokepoint for domain registries such as .com, .net and others. However, this privately held body has so far only chosen to apply its authority on behalf of trademark holders. The recent bitter fights over who would be granted the domain of .vine and .wine saw France lash out against ICANN, and India too expressed its concerns at private companies being awarded domains like .indian and .ram, for fear they could be misused. Another 'choke point' is the root server, which serves as the registry for domain names. Who maintains these is a pertinent question. For example, VeriSign maintains the .com and .net root servers, and is based in Virginia, USA. Therefore, that is where its jurisdiction lies. More recently, some root servers have been distributed across multiple jurisdictions, making it harder to locate and attack. However, keeping these root servers under one authority such as ICANN is seen as crucial to many, as it allows web users based in different countries to 'talk' to each other. While countries can create a parallel internet system, as China and Russia have done, it would mean that users across the world would have to modify their computers to point to the alternative DNS rather than ICANN DNS. This is seen as a serious affront to the seamless nature of the current, dominant, internet experience.

Ultimately, the book is an examination of trade and law, and its new avatars in the cyber realm. A new

global division of labour – where US legal documents are being prepped by lawyers based in India, and phone calls to big American companies are being answered by Filipino workers – also means countries will display protectionist behavior. For example, in the light of increasing medical images review (including radiology)moving from the US workforce to India, the US Congress restricted Medicare reimbursements for services that were subcontracted to providers located outside the country. This dichotomy between wanting free trade but protecting ones country from the same has come up during Trade 1.0 and continues to be a theme in Trade 2.0

Chander also flags newer scenarios that are emerging. For example, 'cloud computing' is essentially the act of 'moving a computer service to remote computers, typically with the user both largely unaware of the jurisdiction or jurisdictions from which the service is actually supplied.' This is important. For companies such as Google, the cloud exists across various techno-legal-economic jurisdictions, which he fears could become a 'legal black hole'.

The legal aspects of this new silk road,and how they should be shaped, form the crux of Chander's book. After going into some detail about one of the biggest companies to exist thanks to the internet – cheekily called Facebookistan due to its billion *citizens* – Chander quotes founder Mark Zuckerberg acknowledging its special role: "We exist at the intersection of technology and social issues." But what has this meant? Differing privacy standards across the world, where facial recognition features might not be welcome in some regions as they are in others; differing free speech environments where governments might want to step in to censor content their believe is inflammatory; and different regulatory climate with some states moving to tax Facebook on its growing advertising revenues.

What does this lead up to? A few steps are outlined by Chanderto ensure trade across cyberspace remains 'free'. The first is legal glocalization – where sites are localized to conform to varying rules in different jurisdictions. However, Chandertempers this suggestion, warning that excessive interventions will hamper the worldwide nature of the web. This scenario harks back to an earlier question – whose law applies? The choices here are the following: country of origin; country of reception; UN or a treaty-based law; self-regulation by the private companies involved and finally, user-based regulation. There are problems with each scenario. The country of origin suggestion might spark what is called a 'race to the bottom' with companies trying to register themselves in places with minimal regulation. An international treaty seems difficult, given that speech, privacy, defamation and a few other concepts are difficult to create consensus around. The country of reception principle would make it very difficult for corporates trying to enter many different markets, and both regulation by users and/or the companies themselves might lead to problems later, given that consumers often lack knowledge about the services they use. All these problems lead Chander to suggest adopting the principle of 'harmonization' where one should imagine a regulatory 'race to the top'; with regulatory competition among countries leading to a global welfare-maximizing ideal. This, coupled with companies abiding by the 'do-no-wrong' principle – for example, not assisting authoritarian regimes to suppress free speech and human rights –would help countries across the world reach their goal to manage overlapping jurisdictional authority. Courts could decide on applicable jurisdiction according to the state with the closest connection to the dispute. The creation of international standards and the increasing difficulty of enforcing differences would, according to Chander, encourage the emergence of global best practices.

Chander's book is a knowledgeable and a timely intervention in a world increasingly relying on the information society to move it forward. India too, speaks the language of 'Digital India' and everywhere one looks e-commerce websites are capturing the public imagination. Start-ups are the order of the day; complementing the already established IT services industries. Global commerce is changing the world, and the internet is now termed a 'global commons' – it has achieved as much importance as the seas and space! In this scenario, some of India's own unique problems in this domain are addressed by this book: that of jurisdiction over transnational data flows. In the past, Indian ministers have offered the opinion that jurisdiction should extent to the country of reception. Currently, India is exploring the idea that data flows

originating and ending in one jurisdiction should only be routed through that country, and not through international servers. This does not address the problem of jurisdiction of international data flows, but it is a start. Further, India believes that the routing of internet traffic and their numbering need not be carried out by a private body such as ICANN, but that the role can be shared by governments under bodies such as the International Telecommunications Union. These are suggestions on the table, but strike at the heart of the debates being carried out about the future of the internet – which is also the future of international trade.

There is only one weak point in the book. Chander wonders if international trade law could encourage political freedom around the world. Human rights in cyberspace do end up in debates about not the production, but the consumption of knowledge. Many in the West want the internet to adopt common values of free expression. Yet, this can often be the point of departure for many countries. Some are authoritarian and want to impose censorship. Others, and India can fall into that category, is not interested in foreign elements dictating national policy. This is the reason why foreign funded bodies often come under the scanner in India. The argument is tricky, and opens up more questions than what this book seeks to answer.

Ultimately, Chander's informative book engages the reader. It is recommended for those who want to peek into the nuts and bolts of the internet, understand the application of the law that guides it, and finally, follow the smell of money!

The author heads the Cyber and Media Initiative at the Observer Research Foundation.

When is Personal Info Fair Game?

Anahita Mathai

In late November, Sony Pictures Entertainment was hacked by a group calling itself the 'Guardians of Peace'. Within a few days, the magnitude of the leak became clear. In the 100 terabytes of data stolen were unreleased movies, private correspondences, employee information including medical and financial data, and much more. Speculation was swirling that North Korea had initiated the attack as retribution for the Sony film The Interview, about an attempt to assassinate North Korean leader Kim Jong-un; these rumours were later endorsed by a Federal Bureau of Investigation (FBI) statement. There was no question about publishing the news that Sony's systems had been breached, and many news outlets worldwide did. However as the nature of the information leaked became clear, decisions about publishing that information became decidedly more complicated.

The initial lots of information leaked contained salary information for several thousands of Sony employees, notably the top 17 executives of the company who were making more than 1 million US dollars a year. The information about the top executives was widely disseminated, as it revealed some startling statistics about Sony pay grades. The top executives were overwhelmingly white and male – there was only one woman and two non-white execs. This was still 'safe' information to publish, since it spoke to important issues: the lack of diversity in the upper echelons of an industry leading company, and the pay disparity between male and female employees with the same or similar titles. Additionally, much of the information could be found legally elsewhere, in public tax disclosures. It took the leak to bring this information front and centre.

Then the email-floodgate opened. Emails between and about top executives and celebrities began doing the rounds, exposing both mundane production details and the salacious gossip of star-studded feuds. Several sites noted that people were drawn to the information because the glamorous veneer of Hollywood was being lifted, and the mysterious workings of a secretive industry revealed. Some of the emails revealed what could be critical information about industry attitudes, like the exchange between a Sony exec and a producer about President Obama's favourite movies, naming only 'black' films. Many were published simply to embarrass the big names mentioned within them.

The timing of the Sony hack, so soon after 'the Fappening' in which private, nude photos of celebrities were leaked online, drew inevitable comparisons between the two. The hacking and leaking of the nude photos was almost universally decried, and news outlets did not publish the photos. Those who did not approve of the Sony information being revealed declared that the two incidents amounted to nearly the same thing: leaking private information to harm another party. This ignited a debate about whether the Sony emails were more newsworthy, and closer in fact to Wikileaks-style information leaking and the Snowden revelations.

Clearly the information from the Sony hack lies somewhere in the middle: more newsworthy and noteworthy than nude photos, but perhaps not as much in the public interest as national security concerns. The differences have to do with how the information was obtained in each case, and who the targets were. The information in all three scenarios was stolen, but were those thefts justified? The celebrity photos were gleaned from hacking individual iCloud accounts, the Sony emails from corporate servers, and the Snowden leaks from databases of the United States government itself.

The hacking of personal accounts to leak private photos, of celebrities but in their private capacities, is perhaps the most clear-cut case. The nature of the photos, nudes of mainly young women and couples, added to the gravity of the crime, with some saying it

was akin to a sexual violation. When Sony was hacked, despite the fact that the hacks were of information pertaining to individuals, there was still a sense that the company itself was the target. It is perhaps easier to sympathise with an individual, even a rich and famous one, than with a faceless corporate monolith or the might of the state. There is also the sense that the larger the target, the better prepared it should have been for attacks such as those perpetuated – where were the safeguards?

Those who initiated the hacks acted illegally, but what about the journalists using that information? In the United States journalists are protected by the First Amendment which allows the use of such information to educate the general public. Furthermore, it could be argued that Sony could no longer consider the information private anyway. Can the information gleaned from the hacks be distinguished from other information of dubious provenance? Journalists use information from anonymous sources and whistleblowers as a matter of course. They also use information which their targets would prefer remained private. Does this make journalism a form of 'permissible thievery'? It may be a question of interpretation rather than access. The FBI approached at least one cybersecurity expert to question him about 'illegal downloading' after he had accessed the leaked documents. Sony itself tried to disrupt downloads of the stolen files. Yet there seems to be no stopping the flow of information.

With such massive amounts of information, as in the Sony hack case, the Snowden files and the Wikileaks, people have to make calls about what information is interesting and in the public interest. Are experienced journalists the best people to make those calls? Researched articles with an editorial stance of some kind are surely better than simple reproductions of stolen material online. Journalists can provide context and verify information before publishing it. However, in publishing stolen material, journalists run the risk of playing into the hands of the hackers. If the Sony hack was conducted to harm Sony financially, aren't journalists helping this cause by reporting harmful details about the company? On the other hand, do they have any obligation to protect Sony? There is perhaps no way to stay impartial when reporting information of this kind. Some feel that in the current environment, journalism itself is under threat, with the 24-hour news cycle and changing modes of publication. Any publication that claims to carry news cannot afford to be left out of a story this big.

The author is a Junior Fellow with the Observer Research Foundation.

The future of the internet is up in the air

Alex Pearlman

The internet as you know it is about to fundamentally shift. While Americans are embroiled in debates over net neutrality (watch John Oliver explain it) and data surveillance, little attention has been paid to issues that affect global internet security as a whole. Big changes are ahead, and there's been a surprising lack of discussion about how the web we've come to know and love will be managed, and who will be at the helm.

The organization that currently maintains the easy global flow of the internet, the Internet Corporation for Assigned Names and Numbers (ICANN), is about to be released from under the US Department of Commerce. Since 1998, ICANN has been operating the global domain name system from within the US government, including setting policy and managing the functions of root name servers. But that's all about to change.

The nonprofit, which is based in California, has become too big and too important to be under the sole control of the US, and so in September 2015, ICANN will emerge as an independent entity – if they can conceive and implement a system of accountability that the US agrees to.

In an attempt to create a system through which everyone who uses the internet has a say in running it (democratic principles being one of the internet's founding ideals), a conference was convened in Sao Paulo, Brazil in April to discuss how the international community might come together to govern the internet.

The NETMundial Conference brought thousands of groups together to discuss how they might implement a "multi-stakeholder" model of governance, through which countries, corporations, NGOs and citizen experts would all have a say in global governance of the internet.

ICANN is leading the charge to create an international body that would be tasked with not only maintaining the technical elements of the performance of the internet, but would also address questions of global internet governance and accountability, and create a mechanism to levy and enforce sanctions.

With a looming deadline and thousands of groups all trying to insert their opinions – from liberal nonprofits to the government of Uzbekistan – the task is a daunting one.

ICANN's best idea so far has been to create something akin to "a United Nations Security Council of the internet." By setting up a "coordination council" with 20 members and 5 permanent seats, this body would channel concerns through a multi-stakeholder panel made up of delegates from civil society, nonprofits and technology corporations, as well as state representatives.

It sounds ideal. But can something so complicated come so easily?

Already there are cracks in the foundation and a schism looming between long-time internet governance nonprofits and the countries and corporations that want more control. It's a tug-of-war that has a firm deadline, and the players are all scrambling to keep up.

Uniting for internet freedom

Experts at the Centre for International Governance Innovation (CIGI), an Ontario-based think tank, have been studying the ICANN dilemma. The group's research suggests that the public approves of the proposed multi-stakeholder system: In a 2014 survey of more than 23,000 people of all ages in 24 countries, CIGI found that 83 percent of internet users believe access to the internet is a basic human right and 57 percent agree with the multi-stakeholder model.

"People see the internet as critical to their own livelihood, freedom of speech, knowledge awareness, and almost a vital instrument of not just communication, but

also increasingly economic survival," said Fen Hampson, director of CIGI's Global Security and Politics Program. "It's reflected in the simple question: do you think it should be a human right?"

Even users in Tunisia are in favor of the multi-stakeholder model suggested by ICANN, NETMundial and CIGI. The Tunisian government has a history of tough internet censorship laws, and the country's status has only recently been upgraded from "not free" to "partly free" in Freedom House's annual Freedom of the Net Index.

"Were an intergovernmental body like the UN to take up a role in running the internet at a global level, key decisions would be taken by the same telecommunications ministers that restrict online freedoms at home [in countries like Tunisia and Egypt]," said Adrian Shahbaz, internet freedom researcher at Freedom House, a US-based advocacy group.

Shahbaz emphasized the value of having a variety of collaborators – not just government officials – make key decisions on how to run the internet in an environment that fosters accountability, transparency and a commitment to free speech and human rights.

Bumps in the road

Not everyone shares the positive outlook that many governments seem to have. Prominent internet freedom advocacy organizations have said that the very notion of a council goes against the principles of a free and transparent internet. Some have come out forcefully against the idea, saying it's too much of a top-down structure and isn't inclusive enough.

However, the clock is ticking, and CIGI believes it's better to get started and adjust as needed.

"The bodies that have been charged with looking at this have been spinning their wheels, because some people have some very ambitious ideas about corporate governance, and there are governments in the mix who want greater control," Hampson said. The NETMundial model is "the best the way to deal with the transition issue: it's simple, it's elegant, it's more politically feasible than the other options," according to the CIGI team.

But even Hampson acknowledges that ICANN's plan is not foolproof. To push through, he said, the plan must "pass the political smell test": the US government has to agree with it.

"At the end of the day, we have to recognize that the US has a veto and they have to be happy with whatever is being proposed," Hampson said.

CIGI's Gordon Smith pointed out in a recent interview that some large American corporations – even ones who have been historically unfriendly to the idea of net neutrality, including the Motion Picture Association of America (MPPA) – "did very well [at the NETMundial Conference] and had a good outcome, a result in their favour."

Other stakeholders, such as the UN-affiliated International Chamber of Commerce and the Internet Architecture Board, who oversee the influential nonprofit Internet Engineering Task Force (IETF), have come out in recent weeks slamming both the NETMundial coordination council plan and ICANN. IETF, via the Internet Society, also issued a statement of dismay. Citizen participants, many of whom recall the last time corporate organizations tried to get involved with internet governance – remember SOPA? – aren't overjoyed, either.

The lack of support is a significant dig at the present initiative on the table. In particular, the International Chamber of Commerce, as the United Nations' horse in the race, should have been easy to get on board. The fact that they're backing away doesn't bode well for ICANN's plan.

Over at tech gossip site The Register, blogger Kieren McCarthy has accused ICANN of "building castles in the sky." The Internet Architecture Board and the International Chamber of Commerce have issued letters that said respectively that they will "not participate" and "cannot endorse" the plan as it currently stands.

So what's next? Where does ICANN go from here, and can a plan for international internet governance be salvaged before September?

"Building bottom-up governance processes is one of our highest priorities with respect to governing ourselves on the Internet," Internet Society president and CEO Kathryn Brown wrote in a blog post Sunday. Brown also called on the internet governance community to carry through on earlier promises "join forces" and create solutions through open dialogue.
A meeting set for Dec. 17 with ICANN's CEO is set to include representatives from the leading internet governance NGOs and other advocacy groups. There will likely be a compromise on the question of the coordination council and how to move forward with more popular support. No matter what, without these groups on board, ICANN faces the greater challenge of convincing the public that the internet won't just be controlled by a bureaucratic hierarchy of governments and corporations.

This article originally appeared on GlobalPost.com

The author is a digital journalist and editor who reports on global human rights, with an emphasis on women's issues and internet freedom.

ESSENTIAL READINGS

COMMENTARIES

Kim Zetter," The Evidence That North Korea Hacked Sony Is Flimsy", *Wired*, December 17, 2014

Nathaniel Beach-Westmoreland, "If North Korea Did Hack Sony, It's a Whole New Kind of Cyberterrorism", *Wired*, December 23, 2014

Dominic Rushe, "Privacy is not dead: Microsoft lawyer prepares to take on US government", *The Guardian,* December 14, 2014

Michael Cieply & Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm" *New York Times*, December 30, 2014

Doug Bandow, "'Punish' North Korea For Cyber Assault: Recognize Kim Jong-Un And Give Pyongyang Some Benefits To Lose", *Forbes*, December 20, 2014

JOURNAL ARTICLES

Aditya K Sood & Richard Enbody, "U.S. Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers", *Georgetown Journal of International Affairs*, December 2014

Michael N Scmitt and Liis Vihul, "The Nature of International Law Cyber Norms", *Tallinn Papers No. 5 (NATO Cooperative Cyber Defence Centre of Excellence)*, December 1, 2014

Morteza Vesali Naseh, "Person and Personality in Cyber Space: A Legal Analysis of Virtual Identity", *Social Science Research Network*, December 2014

Stuart Malawer, "Challenging Chinese Economic Cyber Espionage with WTO Litigation", *252 New York Law Journal No. 120 at 4*, December 2014

Ashley Krenelka Chase, "Neutralizing Access to Justice: How the Demise of Net Neutrality Hurts Prisoners the Most", *Social Science Research Network,* December 2014

REPORTS

Lee Rainie and Janna Anderson, "The Future of Privacy", *Pew Research Foundation Internet Project,* December 18, 2014

Urs Gasser et al, "Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse", *Berkman Center Research Publication No. 2014-17*, December 15, 2014

James Lyne, "Security Threat Trends 2015", *Sophos*, December 18, 2014

BOOKS

Alan Chong and Faizal Bin Yahya eds, *"State, Society and Information Technology in Asia"*, Burlington: Ashgate Publishing Company, December 2014

Speech by Markus Ederer, State Secretary of the Federal Foreign Office, Germany, at the Global Cyberspace Cooperation Summit

Berlin – December 4, 2014

Bruce McConnell,
Excellencies, Ladies and Gentlemen,

It is a great pleasure to have you all here at the German Foreign Office.

I would like to extend a special greeting to the principals and team members of the EastWest Institute, co-host of this important 2014 Cyber Cooperation Summit. And I have the sad obligation of paying homage to the late John Mroz, who for so many years guided the EastWest Institute.

No welcome would be complete without acknowledging the contribution of the sponsors. Today, you are playing a double role: Not only does your generosity make this conference possible, but as representatives of the IT industry and of civil society, you participate as essential stakeholders in Internet affairs.

Allow me to share with you some thoughts that show how the internet also changes us foreign policy players in our day-to-day work, in our actions and reactions and in the way we communicate with our stakeholders.

My first reflex when describing the Internet would be: Opportunities

A few weeks ago, Germany's leading internet news site, Spiegel Online, published a remarkable op-ed. piece: A sixteen-year-old described how, for the first time in his life, he bought and read a paper magazine. From his writing, he appeared to be a well-educated, articulate and thoughtful young man -- in fact, he bought the magazine because it contained a special on the macroeconomics of market economies, or, as he called it, "capitalism". Yet this young man had never before had the urge to obtain or read a print product. All his information he got online.

To me, this story indicates to what extent the Internet changes our lives.

This is true for individuals as well as for institutions: When I began working as a diplomat, we would get letters from citizens politely enquiring about this or that aspect of foreign affairs.

Today, we have a German and an English Facebook page, a German-language Twitter channel with 210.000 followers and an English-language one with 40.000 followers. And we have plenty of web presences and Twitter channels via our Embassies abroad in Chinese, Arabic and Russian…you name it.

The Internet brought politics closer to the people, made politics more transparent, more responsive, and in a way more democratic.
The Internet has also changed the social fabric in which we live, as we communicate instantly and seamlessly across borders and societies: This is a world of opportunities. And the biggest opportunity will be to create a truly global village.

But the creation of this global village also leads me to my second thought: Challenges

The Internet and cyber technology present dangers, too. In fact, the cyber space is a potential new theatre of distrust and conflict.

Numerous states are pursuing military cyber-capabilities. However, traditional political-military strategies are difficult to adjust to the cyber-space.

During the Cold War, the opposing parties relied on defense efforts as well as arms control and confidence building measures. Such defensive approaches require that the consequences of any attack be clearly

and credibly communicated ex ante to any potential adversary. This can be difficult in cyber-space, where you often have to guess who the adversary is. Uncertainty about the origin of hostile cyber-action is a characteristic of cyber-incidents. As a consequence, the masters of cyber capabilities favor the offense. This introduces an element of dangerous instability into international affairs.

The dependence of the modern world on the Internet also means that cyber incidents can escalate into "real-life" conflict or even war. Consider the following scenario: A country is in a state of political turmoil. Relations with the neighboring state are strained. All of a sudden, the main telephone and internet provider becomes victim to a software bug. Nobody can make phone calls, there are no e-mails. Government, banks, security services are paralyzed. Critical infrastructure is affected. The damage is enormous. All because of some hard-to-detect malware. Who planted it? For what reason? Suspicions run high that the less friendly neighbor perpetrated a cyber-attack. How to respond? The danger of escalation is evident.

Therefore I believe that we urgently need to adapt to this new conundrum of offense and defense – or should I say lack of defense in the cyber space.

A third thought that I would like to share with you is about the question of: Trust

The Internet's importance is developing faster than international politics can react. In principle, the Internet is built on trust, between the providers and the users, the users amongst themselves, but also between governments and their people.

Take it at the most personal level: How much trust does it require for you to post your thoughts and ideas online? A lot – I trust. And now just wonder how much trust businesses need to make production processes Internet-dependent, which is the essence of the "Internet of Things". Then consider how important trust is for states whose critical infrastructure requires safe, secure and reliable IT systems.

There are things we can do on our own: We can make a commitment to protect our IT systems, to make them more resilient. However, to preserve and further develop the global Internet, we have to build and rebuild trust.

Technical solutions, such as chip-based security technology, can help. But they must be flanked by political agreement between all stakeholders on how to ensure that the internet remains open, free, safe, and dynamic.

My suggestion is to use this Cyber Cooperation Summit to explore ways of building and re-building this kind of trust in the internet.

And this brings me to my fourth point: Rules of the road.

Rebuilding trust can be done by agreeing on certain rules of the road that will guide behaviour.

We cannot allow cyberspace to be a rule- or lawless abode. Fortunately, there is an emerging international consensus on this point.

The United Nations General Assembly has confirmed that international law, and in particular the UN Charter, is applicable to cyberspace.

At the same time, there is consensus that state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of cyber activities and to their jurisdiction over IT infrastructure within their territory.

From this starting point, let me propose some rules for the discussion at this Cyber Cooperation Summit:

1) States should not allow IT infrastructure located on their territory to be used for actions that violate international law.

2) States should protect critical information infrastructure located on their territory, and should have adequate cyber security provisions.

3) States should respond to inquiries and appeals for help in case of a cyber-emergency.

4) States must respect individuals' universal human rights "online" as well as "offline".

Let me expand on this last point: Individuals enjoy the same universal human rights "online" as "offline".

This includes the freedom of expression -- including the freedom to seek and impart information --, the freedom of assembly and association, and the right to privacy.

Respect for the right to privacy has proven particularly thorny. May the state collect unlimited electronic data on individuals, and insist that the business community assist in doing so?

We welcome in this regard that just last week, the draft resolution based on a German-Brazilian initiative on the "Right to Privacy in the Digital Age" found unanimous consensus in the Human Rights Committee of the UN General Assembly. We look forward to the resolution's adoption in the Assembly and to the issue being taken forward in the Human Rights Council.

We need to balance freedom and security. That balance needs to be well thought through and made subject of a political discourse, nationally and internationally.
And the instruments of security need to be proportional to the costs they impose on our privacy.

We also need to discuss the collection, storage, processing and analysis of "big data" by private companies. Some firms associated with the use of "big data" are facing critical questions whether they sufficiently respect individuals' privacy rights.

Unless clients are satisfied with the answers, these firms' business may – and I predict: will – suffer.

The European Parliament included this point last week in its resolution on consumer rights in the European digital market, when it called for the swift adoption of the new modernised Data Protection Package. A high level of protection of personal data, user safety and control over one's personal data and a stable, predictable legislative environment in which businesses can flourish, have to be balanced.

The imperative to balance privacy and security leads me to my fifth and last point: Shared interests.

Rules for cyberspace must be complemented by concrete confidence-building measures.

I outlined to you in the beginning the danger of escalation stemming from cyber incidents. A good way of preventing such escalation is to engage in transparency and confidence-building. The Organisation for Security and Cooperation in Europe (OSCE) has made important progress in this field: In December 2013, Participating States agreed a first set of measures to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICT.

It is encouraging that the implementation of these measures has begun, in a serious and workmanlike fashion. This sends an important signal: International cyber security is a common concern. It should be pursued regardless of political differences, in the interest of global stability.

We are looking forward to supporting the new OSCE chair, Serbia, in taking this work forward, and we will do our share in 2016, when Germany will be at the helm of the OSCE.

The EastWest Institute's 2014 Cyberspace Cooperation Summit here at the Federal Foreign Office in Berlin promises to be an important milestone in a multi-annual process. It builds on four previous such conferences, in Dallas, London, New Delhi, and Silicon Valley (2013).

In your work, I encourage you to be as inclusive and interactive as possible. Use the opportunity to exchange views between government, industry and civil society representatives. This may well be a step to build the trust that is so urgently needed.

I wish you all good and fruitful discussions. You are doing a tremendously important job!

Thank you very much.

Source: *German Federal Foreign Office, Information Service*, December 2014

"Joint Elements"

Media Note from the US-EU Cyber Dialogue

Washington/Brussels – December 5, 2014

On the occasion of the inaugural meeting of the U.S.-EU Cyber Dialogue in Brussels, Belgium on December 5, the participants jointly agreed to specific areas of collaboration and cooperation as follows:

International Security in Cyberspace

All participants welcomed the landmark consensus of the 2012-2013 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including the affirmation of the applicability of existing international law to cyberspace. Both sides welcomed the confidence building measures agreed to in the Organization for Security Cooperation in Europe and their implementation in order to build confidence and reduce the prospects for conflict in cyberspace and commended efforts to expand similar efforts in other regional fora such as the ASEAN Regional Forum and the Organization for American States.

Internet Governance Developments in 2015

All reiterated that no single entity, company, organization or government should seek to control the Internet and expressed their full support for multi-stakeholder governance structures of the Internet that are inclusive, transparent, accountable, and technically sound. As such we:

- emphasized the value of the annual Internet Governance Forum (IGF) and encouraged its ongoing improvements in line with the UN Commission on Science and Technology for Development recommendations. Urged renewal of the IGF's mandate and the continuation of its work, according to paragraph 72 of The Tunis Agenda, beyond the end of its current mandate in 2015.
- recognized the importance of the NETmundial Global Multistakeholder Meeting on the Future of Internet Governance hosted by Brazil in April 2014 which set common principles and important values for an inclusive, multistakeholder, and evolving governance framework. Both sides are committed to implementing the NETmundial roadmap.
- welcomed the multi-stakeholder community's engagement on efforts to address accountability of the Internet Corporation for Assigned Names and Numbers (ICANN) and transitioning the stewardship of the Internet Assigned Numbers Authority (IANA), recognizing the positive progress of these two interrelated initiatives.

U.S.-EU Cyber Related Work Streams

They both welcomed the continued cooperation occurring through the existing U.S.-EU Working Group on Cybersecurity and Cybercrime and highlighted the cooperation occurring in the following key areas:

Cybersecurity:

- On public-private partnerships, they noted the preliminary workshop held in November 2014 comparing U.S. Cybersecurity Framework and EU NIS Platform approaches to cybersecurity risk management and voluntary information sharing. Participants highlighted the opportunity for future work to foster common

approaches and best practices to cybersecurity risk management.

- On awareness raising, they highlighted the successful conclusion of the synchronised U.S.-EU cybersecurity awareness raising month in October 2014, noted the progress made in awareness raising cooperation through the Working Group, and looked forward to further cooperation in this area.
- The two sides noted the opportunity for further collaboration among the U.S., EU, and member states on cyber incident management and considered a joint activity with the aim of enhancing cooperation in case of global cyber-incidents, building upon the lessons learned from the U.S.-EU CyberAtlantic 2011 exercise, national exercises, and operational experience.

Cybercrime:

- The Global Alliance Against Child Sexual Abuse Online has consolidated, grown larger and gained new momentum as noted in the Ministerial Conference held in Washington on 29-30 September 2014 and its ambitious Ministerial Statement. We will continue our work together to ensure this initiative is effective and intensify our cooperation to tackle jointly the issues presented by transnational child sex offenders, following the mandate given at the U.S.-EU Summit this year.
- We affirmed our commitment to promote the Budapest Convention as the reference framework for the fight against cybercrime, including by working together in international fora. We welcome the most recent signatories in 2014: Luxembourg, Turkey, and Panama.
- We will also proactively work with Internet organizations (such as ICANN and the Regional Internet Registries) to engage their support and cooperation in furthering greater security and stability on the Internet and to address cybercrime challenges

Upcoming Cyber Events

The two sides look forward to the UN General Assembly ten-year review of the World Summit on the Information Society in 2015. They both believe that the timing of the review is appropriate as the UN General Assembly will be finalizing a post-2015 development agenda, and the review will build on efforts to continue bridging the digital divide. The General Assembly's recognition and allowance for multistakeholder participation in the review was appreciated, and participation from all stakeholders is strongly encouraged and welcomed.

With the increasing relevance that cyber issues play in society overall, the United States and the EU welcomed the upcoming Global Conference on Cyberspace in The Hague in April 2015 and the annual Freedom Online (Coalition) Conference in Mongolia in May 2015.

Promotion and Protection of Human Rights Online

They reaffirmed their strong commitment to the promotion and protection of human rights. They emphasized that all human beings have the same human rights online and offline and that states have an obligation to protect those rights in accordance with international law. In particular, the rights to freedom of expression and privacy, as set out in the International Covenant on Civil and Political Rights, in the digital sphere require the attention of all stakeholders.

Global Cyber Capacity Building

Both sides emphasized the importance of bridging the digital divide towards fostering open societies and enabling economic growth and social development. They reiterated their commitment to an approach to cyber capacity building that leverages the expertise and resources of all stakeholders to ensure that people around the world can fully benefit from the Internet and ICTs. They welcomed further coordination among

actors globally and agreed to continue exchanging views and good practices, as well as seeking future synergies in their respective global cyber capacity building initiatives.

The chairs agreed that they will continue their collaborative efforts and convene the U.S.-EU Cyber Dialogue again in approximately one year's time in Washington, D.C.

Source: *US Department of State, Office of the Spokesperson*, December 2014