CYFY
THE INDIA CONFERENCE ON CYBER SECURITY AND INTERNET GOVERNANCE

ORF CYBER MONITOR

CYFY 2015 14th to 16th October

VOLUME III | ISSUE 5 | MAY 2015 | http://cyfy.org

COMMENTARY

A Time to Lead

Samir Saran & Abhijit Iyer Mitra

India is in a position to shape the cyberspace debate. It must start with the Hague conference. This requires an understanding of its own position, diplomacy and the roles of Indian stakeholders.

India Could Reset Its Position on Internet Governance. Will It?

Mahima Kaul

Several recent developments have altered India's domestic approach to internet policy. What kind of impact will these developments have on how India approaches international policy debates?

Net Neutrality: The net worth of freedom

Karan Lahiri & Chaitanya Ramachandran

The structure of the internet inherently makes it a free and democratic space. A recent consultation paper has raised fears that India's telecom authority wants to create differently-treated zones in that space.

Leave the Internet Alone

Payal Malik & Avirup Bose

The debate on net neutrality is a misnomer of a social movement. Activists are running a misaligned campaign to save the internet with little understanding of the underlying issues.

What Does the Cyberspace Landscape Look Like in the APAC?

Tobias Feakin

Already contending with a tense geopolitical backdrop, there is an urgent need for countries in Asia to cooperate, if not harmonise on cyber security issues and reduce their respective vulnerabilities.

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

Editor: Mahima Kaul

Associate Editor: Anahita Mathai

Governance

The Netherlands played host to the annual Global Conference on CyberSpace (GCCS), with government and civil society participants from around the world meeting in The Hague from April 16 – 17, 2015. Apart from the two days of the conference itself, an entire week (dubbed "Cyberspace Week") was dedicated to side-events and other activities tied to the GCCS.

Consultations were held on issues including norms of cyberspace, international cooperation, capacity building and more. Existing mechanisms were also discussed, particularly those pertaining to the law applicable to cyberspace. More than 30 states attended the Tallinn 2.0 consultation, which builds on the Tallinn Manual on the International Law Applicable to Cyber Warfare. It was of particular significance to the Dutch, with one anonymous official saying that "The Netherlands is a strong supporter of clarifying the application of existing international law in cyberspace…the Tallinn Manual can be a useful source of academic interpretation in this field and the Netherlands was pleased to be able to provide assistance…"

Another official side event, organised by the Observer Research Foundation and the Hague Institute for Global Justice, covered "International Cyber Norms and Global Swing States". It focused on how developing states approach cyber norms and how policy priorities differ for the Global North and South, drawing speakers from both developing and more developed countries.

One notable outcome of the conference was the launch of the Global Forum on Cyber Expertise, which is designed to give "political momentum to global cyber capacity building, make available technical expertise" and provide new avenues of funding for data protection, e-governance and cybercrime prevention. The new forum will be headquartered in The Hague, but operate internationally. More than 40 governments, civil society groups and companies joined the forum at the outset.

Despite these outcomes, some felt that several pertinent issues were not discussed at the GCCS 2015 – most notably mass surveillance. Activists erected a giant inflatable elephant in The Hague, to represent the 'elephant in the room'. Several commentators were disappointed by the fleeting references to privacy and surveillance in the outcome statement.

Previous editions of the conference were held in London in 2011, Budapest in 2012 and Seoul in 2013. At the closing of the 2015 edition, it was announced that the next conference will take place in Mexico in 2017.

Across the Atlantic, another major conference, the RSA conference, was held in San Francisco from April 20-14, 2015. With a focus on security particularly, the conference was attended by more than 500 vendors and security practitioners and also featured high levels of US government participation.

The UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security held meetings in New York this month, raising expectations about their eventual output. The group is building on the landmark report issued by the previous GGE, and is expected to release its own report in June. The group will address questions of capacity building and cooperation in cyber space.

In another indication that companies are backing the Internet of Things (IoT) to be the next big technological revolution, IBM has announced the creation of an IoT division, and a corresponding $3 billion investment. The IoT industry is showing continued signs of growth, particularly in the Asia-Pacific region. It is estimated that there will be 8.6 billion connected 'things' in the

region by 2020, up from around 3 billion currently. If that estimate holds, the industry by 2020 will be worth over $580 billion. This growth comes at a time when researchers have begun work on 'robotic fabric', embedded with sensors, which could lead to responsive clothing for humans or the design of robots not reliant on solid skeletons.

The exposure of the scale of US surveillance at home and abroad, brought to light by Edward Snowden in 2013 continues to have effects around the world. The latest country in the spotlight is Germany; media reports suggest that its foreign intelligence agency, the BND, was collecting confidential information on European companies and delivering it to the USA. At least one of the companies spied upon, Airbus, will be pursuing a criminal complaint against persons as yet unknown. Germany's Interior Minister, Thomas de Maiziere has denied the allegations, saying that currently-classified documents could prove his case. The accusations are particularly damaging for Germany, which reacted strongly to claims that the US had tapped Chancellor Angela Merkel's phone, prompting her to say that "spying among friends, that's not right at all."

After the country's telecom regulatory authority released a consultation paper late last month, the debate over net neutrality and the regulation of over-the-top (OTT) services in India reached a new level of intensity. A pro-net neutrality campaign, Save The Internet!, was launched to rally internet users and convince them to submit their comments to the regulator. Telecom service providers, in their responses, overwhelmingly felt that OTT services should be regulated to the same standards as the regular telecom services they compete with. However, many also came out in support of net neutrality in principle, and suggested that the time was right for regulation in the area. Much of the focus was on 'zero rated' platforms, whereby certain telecommunications service providers teamed up with companies to provide certain services for free. Two in particular attracted a great deal of attention: Airtel Zero and Internet.org. While the consultation is still underway and the regulatory authority has not yet responded to the comments it received – which numbered over 1 million – these two platforms were accused of violating net neutrality in principle. The Facebook initiative Internet.org saw companies which had agreed to join backing out in the face of public opposition. Both Airtel and Facebook's Mark Zuckerberg responded denying that their services were harmful to others in any way. Zuckerberg's response prompted rebuttals which noted that there was a distinction to be made between free internet access and access only to particular content depending on service providers. Internet watchers are awaiting the outcome of the consultation, which could have a significant impact on the way people in India connect to the internet – if they are able to at all.

On a lighter note, India's push for universal internet connectivity has met with an unexpected roadblock: monkeys. The primates are hindering the optical fibre network plan, by eating cables in the state of Uttar Pradesh.

Security

A recently released Pentagon cybersecurity strategy makes clear that the US military is prepared to use cyber operations to "disrupt an adversary's command and control networks, military-related critical infrastructure and weapons capabilities." There has been a shift towards acknowledging cyber weaponry more openly, especially when comparing this strategy report to the last one, released in 2011, which barely mentioned offensive cyber capabilities.

The move comes as the US Congress passed the Protecting Cyber Networks Act, which offers legal protection to companies sharing cyber information with the government. However, the act has been criticised as placing consumer information at risk and offering limited network protection.

The US government is also planning to open a cyber security office in Silicon Valley, which will operate under the aegis of the National Cybersecurity and Communications Integration Center (NCCIC). Opening such an office in Silicon Valley, the hub of cyber-business, is part of the government's strategy to both include private sector players in cyber security operations, and to encourage them to work with the government. Not everybody is on board with increased

cooperation between the private sector and the government, especially given concerns about privacy which have not been fully addressed. Amit Yoran, president of RSA, one of the world's largest computer security vendors, says that private companies – those developing networks and technology – are the best placed to tackle cyber security threats.

Cyber threats are increasing the world over, pushing the demand for cyber security solutions up in several regions. Spending on ICT solutions in the Middle East and Africa is expected to cross $270 billion in the near future, an increase of 29% from last year. The region as a whole is the second-fasted growing cyber security market in the world. Botswana is the latest country to begin the process of establishing a National Computer Emergency Response Team and creating a National Cybersecurity Strategy. They will be aided in these endeavours by the UK government, through the Commonwealth Telecommunications Organisation. US arms maker Raytheon has announced the acquisition of Websense, the network security provider, at an asking price of nearly $2 billion. The buy further highlights the rapid growth of the global private cyber security market.

The Australian Signals Directorate, an intelligence agency, revealed that attacks on Australian businesses and government sites went up by 20% in the last year. It was suggested that the tools for enacting cyber attacks were becoming "more widespread and…increasingly more sophisticated", leading to a game of cat and mouse between security agencies and hackers.

Financial institutions are particularly vulnerable to cyber attacks. To this end, the Securities and Exchange Board of India is developing a "multi-level cyber security framework for the stock market", to shield it from threats internal and external.

Government-sponsored groups are believed to be responsible for most of the attacks on Australia and other countries, with China singled out as a particular culprit. The Chinese government has been linked to a decade-long "cyberespionage campaign targeting governments, companies and journalists in Southeast Asia, India and other countries", which has been singularly effective due to its use of emails in the native language of the recipients, allowing for the spread of malware.

Experts believe that Iran is no longer a 'third-tier' cyber power, having "mastered more techniques of cyber intrusion". Until recently, Iran's cyber capabilities were mainly exercised domestically, with security agencies and government-supported actors facing off against political dissidents and other domestic disruptions. Reports suggest that it was after the Stuxnet worm – believed to have been created by US and Israeli agencies – infected several critical systems, that Iran began to focus on external cyber targets.

Iran has been linked to cyber attacks in the US, including those on the Las Vegas Sands casino, JPMorgan Chase, Citibank and the Bank of America and to an attack on Saudi Aramco which destroyed large amounts of data. As Iran moves away from nuclear weaponry, cyber attacks could prove to be an alternative source of power for the country. Attacks launched from Iranian IP addresses have increased by more than 100% since January 2014. There is evidence to suggest that, sanctions notwithstanding, Iranian companies are "buying IT resources in the West" and using those to launch cyber attacks.

Making a move that could affect millions of internet users, browsers including Google Chrome and Mozilla Firefox will stop "trusting all new digital certificates" that are issued by the China Internet Network Information Center (CINIC). The certificate authority CINIC has been implicated in the issuance of false credentials for several domains including Google.com; users may not now be able to connect to popular sites, including those belonging to banks.

Software obsolescence was identified as a major security risk, particularly to large enterprises. Vendors often fail to provide security patches for 'end-of-life' software, for both cost reasons and as an added incentive for consumers to upgrade. Nevertheless, many users will continue to use this software, and hackers and others are taking advantage of the gap created.

A Time to Lead

Samir Saran & Abhijit Iyer MIter

Today [April 16], Den Hague will be at the centre of the cyber world as over 100 delegations assemble for the Global Conference on Cyberspace (GCCS) hosted by the Dutch government. India's participation at such forums must factor in two important realities of the digital space.

The first challenges the core of how India conducts its diplomacy, a structural bias that seems to repose too much faith in the UN framework. Despite being the principal multilateral institution, the UN represents a legacy arrangement, too slow to govern this dynamic and rapidly evolving medium. It is frequently outflanked by the private sector, bilateral agreements and smart mini-lateral groups pursuing independent agendas. Even in the real world, the UN has been bypassed in Syria, Yemen and Iran, merely agreeing to what formations like the P5+1 decide. On the internet,the "code" is already the "law", where every digital transaction and every user sign-up to a digital service is creating a de jure legal framework that is defining internet governance. Users and industry are determining and enforcing laws like never before, and at a speed that neither nation-states nor the UN is designed to cope with.

The second reality, however, underscores the role of the state in managing the digital commons. India's government must play an active role in formulating the rules for the road, given its social responsibility to ensure equitable access to the one billion "unconnected" citizens for service and governance delivery. But this poses flexibility problems, as governments are incapable of being as nimble as industry or users, and government participation can be both polarising and burdensome. The poser, therefore, is how to retain agency with the government while leveraging the creative capacities outside.

These two factors must be part of any engagement calculus, and responding to them may require India to pursue a policy approach that must have four central features. First, India must seek to deftly institutionalise an "India Exception" in cyberspace through bilateral deals with governments and institutions that manage the internet. One example is how the India-US civil nuclear deal forced an acceptance of India's exceptional status. Similarly, China's bilateral climate deal with the US has ensured that the debate on Chinese baseline emissions has changed dramatically. Such bilateral deals are vital to the pursuit of national interest. They create direction and momentum, which other nations and institutions begin to respond to.

One attractive option for India is to work towards a bilateral "digital economy and security partnership" with the US, free from multilateral meddling and the resultant dilution of interests. Such an agreement creates the critical mass for shaping internet governance. It would bring together two large digital economies already bound by commerce. It would also signal a compact between an incumbent power and an emerging power, between developed and developing nations. If managed properly, this gain can then be socialised through smart mini-lateral arrangements with like-minded countries. This brings us to the second feature.

India should take the lead in setting up a group of experts from 15 to 20 countries in the digital sector to shape internet governance, a proverbial "D-20". Such a forum would translate the key features of India's bilateral agreements into global norms and bring it cyber heft. The chances of entering into effective agreements in line with core interests are far higher at this forum than with unproductive posturing at the UN, where India would have the same weight as, say, Tuvalu. The trick would be to find the correct size and composition with the correct entry parameters, open enough to allow others in as they become relevant.

Third, India should consolidate its leadership by creating ideation forums to shape the discourse, rather than opposing or reacting to others, such as the NetMundial initiative. This could take the shape of a major annual conference or summit, given critical weight by being chaired by the prime minister, and co-convened by the telecom and external affairs ministers. This would also complement the "Digital India" initiative of this administration. Such a platform must be diverse in order to present a more palatable multicolour debate, as opposed to a state-centric position.

Last, to bring all these Indian stakeholders on the same page, an Indian internet governance council must be established. Combining features of the Niti Aayog (digital economy) and a national security advisory board (cyber security), such a platform would bypass the multilateral versus multi-stakeholder debates by organising diverse Indian positions into a comprehensive whole. The government must learn to synthesise domestic opinion like a Swiss knife — common in purpose but different in deployment — so as to allow voices outside government to represent India equally effectively.

Ultimately, India must accept its own exceptionalism. It must thereafter understand how to establish it. India is in a position to shape cyberspace debates, but for that it will need to be flexible, propositional and present everywhere that internet governance is debated. Its strong and diverse contingent at The Hague is a good beginning.

The authors are researchers at the Observer Research Foundation.

This article originally appeared in the Indian Express, April 16, 2015

India Could Use Its Historic Free Speech Judgement to Reset Its Position on Internet Governance. Will It?

Mahima Kaul

"The global can never become meaningful unless it is linked to the local," said Ravi Shankar Prasad, India's Information and Technology Minister, speaking at 2014's Cyfy Internet governance conference. For India, local is a billion aspirations. Local, in 2015, implies a constituency that carries greater demographic weight than Europe and the United States combined. Local is 800 million mobile phones, 140 million smart phones and 173 million Internet connections and growing. His statement begs the question—what is going on in India?

There have been five developments that have altered India's domestic approach to Internet policy since the Minister's statement. A closer look at these developments could provide some insight into how India should approach international Internet policy debates.

The first development is the historic March 2015 judgment by India's Supreme Court, which struck down Section 66a of India's Information Technology Act. Section 66a, widely criticized as restricting freedom of expression online, prohibited anyone in India from sending messages using a computer or communication device that could be deemed "grossly offensive," contained "false information," or which could "cause annoyance or inconvenience." This victory, championed by young lawyers and Internet activists, has emboldened not just the small expert pool of people working on Internet policy issues, but also encouraged a wider audience to start participating in Internet debates.

The immediate effect of this new wave of engagement has led to the second development: the public's unprecedented response to a consultation paper issued by the Indian Telecom Regulatory Authority seeking comment on the regulation of over-the-top services (e.g. multimedia content like Netflix that travels over lines provided by telecoms). Much like the net neutrality debate in the United States, the debate has pitted the telecom industry and some of the larger Internet companies against smaller players and public sentiment, which favor net neutrality.

The third development is the reconsideration of the role of Internet intermediaries in India. Section 79 of the Indian IT Act requires Internet intermediaries to take down content at the behest of a third-party complaint. In light of the recent Supreme Court decision, editorials have begun to appear in leading papers pointing out that blocking, intermediary liability and freedom of expression concerns need to be further balanced to avoid abuse.

The fourth development is the government of India's decision to use open source software for all its applications and services, in order to bring transparency to the government's IT procurement process and tackle corruption. The government believes that the ability for anyone to modify the source code of open source software will allow the tailoring of applications to local needs, royalty free. The policy does, however, leave the door open for proprietary software should open source not be available.

The fifth development is the Indian government's ambitious "Digital India" plan. The plan aims to ensure the delivery of e-governance services to all, build digital infrastructure to enable Internet access, create jobs, and finally, increase electronics manufacturing in India. Interestingly, the government's press release launching the plan refers to digital infrastructure as a 'utility' for every citizen, specifically aimed to deliver high speed Internet to villages, enable "cradle-to-the-grave" digital identities, facilitate mobile banking, create a shareable private space on a public cloud and finally, provide cybersecurity.

Freedom of expression, network neutrality, intermediary liability, open source software and a commitment to provide digital infrastructure as a utility to citizens have all become key points in India's digital journey. For each of these, a uniquely "Indian" model will have to be sought. The absolutist notion of online free speech held by many U.S. proponents cannot translate to India. Further, India cannot blindly adopt network neutrality rules in a market where almost eighty-five percent of its population lives in the shadow of the digital divide, and may well permit Internet providers to offer services that allow for cheap online access by exempting certain traffic from data caps, a policy known as zero-rating. For emerging countries, accessing and building digital infrastructure are pressing questions, as much as it is important of putting principles like freedom, privacy, development and diversity, among others, into practice. Despite not being a signatory to the NetMundial principles, India, in effect, seems to be building a digital society that subscribes to those very values, in its own unique ways.

Suggesting a UN Committee on Internet Related Policies to handle Internet governance, looking to the International Telecommunication Union to absorb Internet public policy issues and even refusing to officially support the NetMundial Multistakeholder outcome document will undoubtedly remain key moments in India's international engagement on Internet issues. But it is time to move forward. India must play a leadership role in the development of global Internet policy. The government needs to respond to the demands of its citizens and reset its position on international Internet governance issues, in line with the progressive developments that have occurred at home. In essence, India should be doing a better job at linking the local to the global.

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

This article originally appeared on the Council for Foreign Relations' Cyber Blog, April 20, 2015

Net Neutrality: The net worth of freedom

Karan Lahiri & Chaitanya Ramachandran

The structure of the internet inherently makes it a free and democratic space. It has fuelled innovation, and is used by millions —about 40 per cent of the global population—to express themselves, absorb multiple viewpoints, and, in some cases, dissent and disagree vehemently, not only with one another but also with the governments that structure their lives in the physical world. It has fuelled revolution, allowing the artist Ai Weiwei to protest against the travel ban imposed on him by the Chinese government, by putting up a picture daily on Instagram of flowers in his bicycle basket. Elegant and effective, much like the internet.

The Telecom Regulatory Authority of India (TRAI), however, wants to create fences within this free space and treat each zone of the internet differently. What is at stake is 'network neutrality'—the idea that telecom companies (telcos) and Internet Service Providers (ISPs), which function as gatekeepers to the web, shouldn't be permitted to discriminate between different types or sources of content. It is an important idea for all of us, and it is certainly worth your time if you want to engage freely on the internet.

Late last month, TRAI released a 'Consultation Paper on Regulatory Framework for Over-the-Top (OTT) services'. While posing 20 questions on internet regulation, and giving one short month as response time, the 118-page long paper advocates imposing an unwieldy regulatory framework on internet services (think YouTube, WhatsApp, Skype, Facebook or any other online service), which it refers to using the loaded term 'Over-the-Top' services. The paper is a response to sustained complaints from telcos that popular apps like WhatsApp and Skype are eating into their SMS and voice revenues. However, it conveniently glosses over the fact that this shift in consumer preference is creating white-hot growth in revenues drawn from mobile internet plans *for the same telcos*! One needn't go further for proof of this than the most recent earnings reports of Airtel and Vodafone, which show impressive growth in revenues from data services (74.3 and 70 per cent, respectively). Clearly, telcos are not in dire straits. So what is motivating them? First, their inability to compete with innovative online services compels them to demand that the regulator hinder their growth. Second, their desire to extract payments from internet companies or consumers of these services, as Airtel threatened to do last December by charging a higher fee for VoIP apps like Skype.

For anyone who has read TRAI's paper closely, the writing on the wall is clear. It recognises that telcos may also discriminate between different apps or services using subtler mechanisms such as throttling online services that hog bandwidth (like the US- based ISP Comcast did with traffic on the popular filesharing service BitTorrent) or compete with the telcos' own offerings (imagine your telco slowing down delivery of free WhatsApp messages, pushing you towards expensive, text-only SMS). Or, as with the recent deal between Airtel and Flipkart, telcos may create a 'walled garden' of services that users may access free but only include those that can afford to pay a hefty entry fee. The paper clearly shows that TRAI is seriously considering a new regulatory structure for online apps and services that endorses this kind of discrimination by telcos.

If all this sounds scary, it's just a glimpse of the future that telcos want to create for the internet, where they are free to arbitrarily charge consumers extra fees (above basic subscription charges) for using assorted online services. This is the future that 'net neutrality' rules would protect us against, by prohibiting telcos and ISPs from discriminating between different types of content. Net neutrality historically began not as a law or rule, but a core design principle of the internet—that the network would make the 'best effort' to transmit all packets of data from origin to destination, regardless of content. But as telcos grow bolder in their intention to stand this principle on its head, many have

begun calling for the enactment of net neutrality regulations.

For most of us, it isn't really the money that is an issue. It is freedom. What net neutrality regulations really seek to protect are two key freedoms cherished by all democratic societies: the freedom to innovate and, more fundamentally, freedom of expression. By ensuring that telcos can't 'pick winners' on the internet by choosing to support some online services while hampering others, net neutrality would ensure a level playing field where startups can go head-to-head with established internet companies in their battle for users. By ensuring that telcos can't control what we say, see, or hear on the internet, net neutrality would protect the freedom of expression and prohibit private censorship of the internet.

TRAI's paper shows a worrying sympathy for the telcos' supposed plight. For example, it repeats the old complaint that while these companies bear the cost of investing in infrastructure to meet demand, online apps and services have no such obligation and should be subject to the same regulatory regime as they are. This argument perpetuates the ludicrous myth that internet access is a zero-sum game between telcos and online services, and misrepresents the regulator's job, which is to protect the public interest. To argue that online services should be licen-sed like telcos is effectively to penalise services that have nothing to do with telecommunications (like YouTube), simply because telcos are worried about being unable to keep up with demand for—or compete with—the online services that Indian users like to use. If telcos are hamstrung from investing in better networks, the solution isn't in regulating online services that drive demand for internet access. To use law professor Tim Wu's analogy, building networks at the expense of network applications is 'akin to selling a painting in order to buy a better frame'.

The internet isn't meant to be a golden goose for telcos and ISPs. The structure on which the network is built is a public resource that telcos (as licensees) hold in trust for all of us. This isn't a novel idea. The Supreme Court actually said this in a decision that telcos would much rather forget—the famous 2G judgment. The principle that the Court has established is that the Government cannot allow the commercial interests of telcos to trump public interest in administering this public resource. That being so, the Government cannot endorse an alteration to the structure of the internet that is to the detriment of consumers merely because telcos claim they are not making enough money.

Let's now come to grips with why 'public interest' hangs in the balance. TRAI's consultation paper is trying to create a regulatory structure through which private players and (potentially) the executive Government can indulge in content discrimination on the internet. Let's assume that *Open* magazine, in keeping with its tradition of brave and unbiased journalism, publishes a piece that implicates telcos in a corruption scam involving the Government. If net neutrality is done away with, it would be possible for telcos to charge subscribers higher rates for accessing the magazine's web-site, just because they can. Alternatively, it can throttle speeds when a user accesses *Openthemagazine.com*. Simultaneously, say, Magazine X publishes views that favour telcos and the Government. Access to Magazine X's website can be made fast and free. In effect, *Open* will be penalised for its speech in a manner that impacts its readership, while users seeking access to such views will have to either pay extra or suffer slow speeds. This is no different from paying a fine or suffering a disadvantage for wanting to access a particular viewpoint. In this hypothetical case, *Open* is being arm-twisted into publishing material that the powers-that-be (telcos and the Government) approve of, just as users are being pushed to access the same favoured content. In a world without net neutrality envisioned by TRAI, criticism can be effectively choked, as telcos becomes censors, making it easier, in turn, for the State to censor the web through its control of telcos.

What if telcos say their intention is only to maximise revenue? After all, they may say putting a price tag on certain forms of online speech isn't censorship but merely a way to pay for the infrastructure that lets users access it. This disingenuous explanation ignores the fact that, for the purposes of the Constitution, a ban is just the same as a monetary levy, so long as the 'direct effect' hinders free speech. When market- based methods have the effect of curbing the dissemination of disparate viewpoints (especially when the methods are

discriminatory), they violate Article 19(1)(a) of the Constitution of India.

Also, it is our right as citizens to access information on the internet without impediment, and to speak across different online forums without hindrance. All viewpoints and forums for expression are to be treated exactly the same. India's Supreme Court has clearly stated that when it comes to freedom of speech, 'it may be the duty of the State to ensure that this right is available to all in equal measure and that it is not hijacked by a few to the detriment of the rest'. In a separate case, the Court also insisted that the public has the right to access differ-ent viewpoints in order for people to have a 'complete picture before them and not a one-sided or distorted one'. In short, no one should be allowed to game the system and manipulate the 'marketplace of ideas'.

Thanks to a popular online movement facilitated by *Savetheinternet.in*, TRAI has been bombarded with emails from ordinary users, opposing the dilution of net neutrality. Some 150,000 people have signed up on the parallel *Change.org* petition, and the number continues to grow. We hope that TRAI will change track and recommend affirmative net neutrality rules. If so, it will join regulators from other countries (like the US Federal Communications Commission,which recently adopted new net neutrality rules) in helping a global consensus emerge on net neutrality. If, instead, TRAI's recommendations fructify into regulations that allow discriminatory treatment of content, we hope that the net neutrality movement that has begun on the internet continues to resist it and takes the matter to Court, to safeguard the integrity of the internet as a medium of non-discriminatory creation and expression.

Karan Lahiri is a litigator and Chaitanya Ramachandran a technology lawyer. They are both based in Delhi.

This article originally appeared in Open Magazine, April 17, 2015

Leave the Internet Alone

Payal Malik & Avirup Bose

The debate on Net neutrality is a misnomer of a social movement. Open Internet evangelicals—from economic polemics and consumer advocates to stand-up comedians—are running a misaligned campaign to save the Internet with little understanding of the underlying issues. The movement, although popular, lacks economic rationality.

Why should telecom companies, after spending millions to acquire scarce spectrum and after indebting themselves substantially to build telecom infrastructure while facing severe price competition, now be retrospectively saddled with a regulatory obligation that restricts reasonable forms of network management.

The acquiescence of the department of telecommunications and the Telecom Regulatory Authority of India (Trai) would signal a new era of retrospective regulatory terrorism—imposing new business costs, hampering the government's commitment to ease of doing business in India.

A recent study by the New York University concluded that Net neutrality would cost Americans 500,000 jobs and $62 billion over the next five years. Trai, without conducting a similar study in India, should be wary of being moved by the populism of the 800,000 emails written to it on the subject.

At the same time, Trai's regressive proposal of licensing over-the-top apps, which are responsible for driving bulk of the traffic to the telecom networks, reeks of an online licence raj—setting bureaucratic entry barriers to the development of this innovative Indian start-up market.

The idea that the Internet should be operated like a public road, carrying all traffic with no discrimination against any traveller, no matter what size, shape or type—is inherently flawed, especially given the present technological limitations of transmitting data on 3G/4G networks, which requires the network to prioritize data.

Moreover, a pure form of Net neutrality as espoused by the open-Internet zealots means Internet services providers (ISPs) cannot sell faster services to businesses or clusters of consumers who are willing to pay, stifling innovation, discouraging investments to better broadband infrastructure and hampering legitimate commercial activity.

It is important to understand that the ISP is mediating between two sides of the market—between the content provider and the final consumer. Upgrades to the network have to be paid for either by consumers or by the content provider or both; nobody knows beforehand what is the right pricing structure between these two sides.

There is no presumption that the right structure is to recover all of the cost of consumer broadband networks from consumers alone and allow the content providers to free ride with zero-priced network access.

A maturing, commercialized Internet ecosystem needs unregulated flexibility to new options for end-to-end connectivity (particularly for new bandwidth and transmission of speed-intensive applications such as IPTV). New bandwidth-intensive applications increase the probability of congestion and degradation of service quality, even in the absence of deliberate efforts by an ISP to throttle bandwidth-hogging subscribers, or to disadvantage competitors.

On the other hand, experiments with zero rating, where some types of content do not count towards data cap may lead to adoption of Internet than otherwise, though evidence of this has not built up, but why presuppose that zero rating is pernicious.

This public road of today's Internet is a result of a continuous process of Schumpeterian innovation, which since the early 1990s disrupted dominant Internet applications, architectures and business models.

The Internet that we experience today is in no grave danger of dying and does not need a government takeover to protect its inherent innovative spirit. Any attempt to impose blanket behaviourial prescriptions to preserve a utopian notion of the Internet's structural integrity disregards the subtle interactions of generation of innovators in their attempt to overcome the inherent limitations of the Internet's protocol stack. Researchers of the Karlsruhe Institute of Technology in Germany curated much of the research literature to date, in a 2013 paper titled *Net Neutrality; a Progress Report*, concluded that experts believe that given the growth of data traffic on the Internet, there are fears that a flood of data will ultimately overwhelm the Internet if proper traffic controls are not allowed. This will lead to congestion problems in peak times, which could only be counteracted by over-provisioning of network capacity, which India currently lacks.

As the Net neutrality debate matures, we suggest adoption of a policy that deregulates the Internet in a manner that allows ISPs to vertically integrate and bundle services, or use traffic differentiation to increase the variety of Internet access and applications to which customers subscribe, all within the contours of India's antitrust laws.

India's antitrust regime empowers the Competition Commission of India to block business activities that harm consumer welfare, restrict consumer choice or deny market access. Such enforcement with a precise enforcement mandate, exclusively targeting objectionable activities, while leaving other pro-competitive conduct that benefits consumers unregulated.

Antitrust analysis with its light touch approach provides a better pedagogic tool to analyse whether particular instances of prohibitions on the ability of network operators to control their vertical relationships would be socially beneficial, rather than a one-size-fits-all regulation, which is much more prone to stifling innovation and deforming the marketplace.

The form of Net neutrality the Indian Twitterati is espousing is an impractical answer to a largely imagined problem. The right approach to keeping the Internet free is to adopt a liberal spectrum regime, along with vigorous enforcement of India's antitrust laws, without the perceived need for prophylactic network neutrality rules.

Payal Malik is advisor and head of the economics division, Competition Commission of India. Avirup Bose is an honorary visiting faculty of competition law at the Jindal Global Law School and a former expert consultant to the commission. The views are personal.

This article originally appeared on Livemint, April 22, 2015

What Does the Cyberspace Landscape Look Like in the Asia-Pacific?

Tobias Feakin

There is no escaping the fact that over the past ten years the Asia-Pacific region has increasingly become a global point of strategic interest and competition. While the United States has renewed its economic and military focus in the region, China has rapidly modernised and expanded its military forces, and tested the boundaries of international norms in the South and East China Seas. Both countries seek to influence nations in the region in order to gain greatest access to Asia's rapidly expanding markets

Set against this evolving strategic landscape, the Asia-Pacific has undergone tremendous political transformation and social change. The development of cyberspace and the information and communications technology (ICT) that powers it has proven to be an integral part of the region's socioeconomic growth.

The online environment is also rapidly growing in importance as an avenue for political and social expression in Asian societies. But technological development in the region varies dramatically. It is home to some of the world's least networked countries, such as Myanmar (1.1% internet penetration) and Cambodia (4.9%) plus some of the most networked, including South Korea (84.1%) and Japan (79.1s%). It also encompasses burgeoning ICT markets such as China and India. Although increasing connectivity has generated undeniable benefits, it has also created new vulnerabilities for governments and the private sector in the areas of national security and online crime. These tensions have manifested differently according to each state's domestic context.

Although increasing connectivity has generated undeniable benefits, it has also created new vulnerabilities for governments and the private sector in the areas of national security and online crime. These tensions have manifested differently according to each state's domestic context. In an environment such as cyberspace where gains are high, the probability of capture is low and deniability rules, many different economic and political confrontations are playing out simultaneously. A by-product of this tension has been a rise in the number of countries that have acquired or are seeking offensive cyber capabilities.

Assessing Cyber Maturity in the Asia-Pacific Region

As connectivity grows, so does the need for cyber-focused policies, legislation and regulatory frameworks. Governments in increasing numbers are starting to address shortfalls in their domestic arrangements, but there are many states that lag behind in either the formation or implementation of cyber-centric mechanisms, frameworks and policy.

To make considered, evidence-based cyber policy judgements in this regional context, there is a need for better tools and information to assess the 'cyber maturity' of nations in the region. In response to this over the past twelve months the Australian Strategic Policy Institute's International Cyber Policy Centre has developed a Cyber Maturity Metric which provides a guide to the regional picture. The UK and the US were included in the study as a benchmark upon which to gauge how well other nations were developing their responses to the challenges and opportunities that cyberspace offers.

Nations' cyber maturity was measured across four different topics, governance structures, military application, digital economies and business, and social engagement. Scores were applied across the different research questions and then a total cyber maturity score was given out of 100.

Most governments across the region are now beginning to understand and prioritise cyber issues as a core tenet of policymaking. While the urgency and thoroughness of how nations respond to the issue varies significantly, all

countries examined in this study are grappling with 'cyber' as a component of state power.

Governance Growth

In the past year, there has been a rapid expansion in many nations' cyber policies and governance frameworks. At the forefront of these policy developments have been India, Japanand Singapore, all of which have introduced impressive-looking policy documents that link together the various departments and agencies with responsibilities for cyber issues.

However, implementing the policy recommendations found in these documents will not be an easy task. At the opposite end of the scale are those nations that lack an adequate focus on their cyber policies, this list includes Cambodia, Myanmar, the Philippines, Thailand, Papua New Guinea, and Indonesia. There's an opportunity for nations that have sophisticated mechanisms in place to help build policy capacity in those nations that are in need of support.

Military Use of Cyber

There are no surprises about which nations are leading the way in the military aspects of cyber capabilities: the US, China, UK, Australia, Singapore and South Korea. However, the increased utilisation of cyber capabilities by the North Korean regime over the past year is a concern.

This has put the South Korean government under pressure to respond to cyber incidents as they arise without an escalation between the two countries, creating another challenge for strategic planners. The onus is on Seoul to develop an ever more sophisticated and mature cyber policy architecture and resilience framework so that it can remain clearheaded in its responses, preventing incidents from turning into large-scale military action in the face of extreme provocation. There's no doubt that we will see increased military cyber developments in the region.

International Engagement

Inevitably the Snowden 'cloud' has hung over the Asia–Pacific region as much as it has over the rest of the world, and this has increasingly had a bearing on the international dialogue on cyberspace. However, a great deal of discussion continues in the region about confidence building measures, capacity building and transparency in the cyber domain, mainly through the ASEAN Political and Security Community.

These discussions present an opportunity for nations to increase their cooperation and mutual assistance in cyberspace. Australia had been at the forefront of international efforts chairing the UN Group of Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in 2013, pushing for a strong practical agenda through ASEAN Regional Forum Workshops, and working hard on practical policing capacity building.

China has also been utilising similar avenues, albeit with different agendas, and its energetic efforts in the international arena cannot go unnoticed. There is a need for nations in the region to coordinate more proactively on cyber issues especially given the wider, sometimes tense, geopolitical strategic backdrop. This environment could potentially see small miscalculations in cyberspace or misperceptions of cyber actions result in extremely damaging consequences.

The author is Director of the International Cyber Policy Centre, ASPI

This article originally appeared on the Royal United Services Institute website, April 24

COMMENTARIES

Zenisha Gonsalves, "Why should feminists care about Net Neutrality?", *The Ladies Finger,* April 23, 2015

Laurence Pitt, "Information Protection & Data Privacy: Taking Back Control", *Symantec Official Blog,* April 8, 2105

Emilio Iasiello, "Huawei and Kaspersky: Are Fears Warranted of Just FUD?", *NorseCorp Blog*, April 8, 2015

Mukul Devichand, "The women of the Chinese internet remain defiant", *BBC Trending*, April 30, 2015

Javier Solana, "Cyber War and Peace", *Project Syndicate*, April 30, 2015

Editorial Board, "Preparing for Warfare in Cyberspace", *The New York Times,* April 28, 2015

JOURNAL ARTICLES

Tamara Bonaci, Jeffrey Heron, Tariq Yusuf et al, "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots", arXiv:1504.04339 [cs.RO], *Cornell University Library,* April 16, 2015

Narelle Clark, "Internet Governance: Is it finally time to drop the training wheels?", *Australian Journal of Telecommunications and the Digital Economy, Vol 3 No 1 Article 3*, April 2015

Jens David Ohlin, Kevin H Govern and Claire Finkelstein, "Cyber War: Law and Ethics for Virtual Conflicts", *Oxford Scholarship Online*, April 24, 2015

Andrew P Geil, "Cyber Security on the Farm: An Assessment of Cyber Security Practices In The Agriculture Industry", *Illinois State University Theses and Dissertations, Paper 158*, April 2015

Lillian Ablon and Martin Libicki, "Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data", *Defense Council Journal, Vol 82 No 2, pp143-152*, April 2015

REPORTS

Don Podesta, "Watchdogs Under Watch: Media in the Age of Cyber Surveillance", *Center for International Media Assistance*, April 2015

Dennis Broeders, "The public core of the internet: an international agenda for internet governance", WRR Policy Brief 2, *The Netherlands Scientific Council for Government Policy*, April 2015

"APT30 and the Mechanics of a Long-Running Cyber Espionage Operation", Special Report, *Fireeye Labs/Fireeye Threat Intelligence,* April 2015

Melissa Hathaway, "Connected Choices: How the Internet is Challenging Sovereign Decisions", GCIG Paper Series No. 11, *Global Commission on Internet Governance/Chatham House*, April 2015

"Cybersecurity Market Report: Q2 2015", *Cybersecurity Ventures,* April 2015

Frederick W Kagan & Tommy Stiansen, "The Growing Cyberthreat from Iran", *AEI Critical Threats Project/Norse Corporation*, April 2015

David G Post & Danielle Kehl, "Controlling Internet Infrastructure: The 'IANA' Transition and Why It Matters for the Future of the Internet, Part I", *Open Technology Institute Policy Paper*, April 2015

"Toward a Social Compact for Digital Privacy and Security", *Global Commission on Internet Governance/Chatham House*, April 2015

BOOKS

Stephen Bryen, Rebecca Abrahams and Shoshana Bryen, *Essays in Technology, Security and Strategy*, Amazon Digital Services Inc., April 26, 2015

David P Fidler, *The Snowden Reader*, Bloomington: Indiana University Press, April 24, 2015

James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis (Routledge Series in Conflict, Security and Technology*, London: Routledge, April 21, 2015

Philip N Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*, New Haven: Yale University Press, April 28, 2015

Shawn M Powers & Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*, Champaign: University of Illinois Press, April 2015

Opening Speech at the Global Conference on CyberSpace, the Netherlands

Remarks by Bert Koenders, Minister of Foreign Affairs, the Netherlands

The Hague – April 16, 2015

Your Excellencies, ladies and gentlemen, Thank you for joining us in The Hague, the international city of peace and justice, at the fourth Global Conference on CyberSpace.

Cyberspace is not commonly associated with fundamental notions like peace and justice. We used to think of 'cyber' as something to do with science, and even science fiction. Books, movies and TV shows, in which computers interacted with humans and with other computers, usually resulting in general mayhem and mischief. And generally these stories presented a dystopian view of the future.

'We are all, by any practical definition of the words, foolproof and incapable of error.' These are the words of HAL, the computer system in charge of operations aboard the spacecraft Discovery One, in Stanley Kubrick's film and Arthur C. Clarke's book 2001: A Space Odyssey.

We no longer need a movie or a book to show us that this statement is not necessarily a comforting one. And even if our systems were foolproof and incapable of error, this hardly holds true for their operators and users.

It's almost in spite of these misgivings that we find ourselves here today. Thanks to modern technology, billions of devices are connected to each other in cyberspace and many more will follow. The Internet of Things is becoming a reality. I don't think it's necessary to laud the opportunities that flow from these developments. Yes, they make our lives easier and our work more productive. They help us relax and engage, entertain and create. But they also make us more vulnerable. The growth in our dependency on digital and online cyber systems is outstripping our ability to safeguard and protect these systems from crime, espionage and infringements on our privacy. And this is where The Hague, as the international city of peace and justice, comes in. Because in the world we are creating, we cannot take peace and justice for granted.

Today we stand at a crossroads. Should we continue to presume that we are as foolproof and incapable of error as we believe our computer technology to be? Should we continue to expect cyberspace to develop, of its own accord, into a realm where peace and justice prevail?

I don't think we should. I believe that the international community, gathered here today and tomorrow, has to find answers to these fundamental questions:

- What are the terms of the social contract that governs the behaviour of citizens, corporations and governments in cyberspace?
- How do we find the right balance between freedom, security and economic growth in relation to cyberspace?

The Netherlands champions a free, open and secure internet. That's our core message. That's what this conference is intended to promote.

- Free, so that everyone has access to the internet and the unprecedented opportunities it offers.
- Open, so that information can flow unimpeded from one user to another, in a single undivided cyberspace.
- Secure, so that personal data are protected and privacy is safeguarded.

We understand that the internet brings people together, generates ideas and so helps shape our

future. The Netherlands is calling for action based on the conviction that we should not curb the innovative power of the internet. And it is calling on governments to closely coordinate their action with all stakeholders, especially the business community and civil society.

I realise that for some of us – especially in government circles – this is not our first impulse. Today, cyberspace is so closely bound up with the way our society works, with the welfare and security of our peoples, that we initially feel governments themselves should take the lead in making multilateral agreements – agreements between states to the exclusion of the private sector and civil society.

But given the nature of cyberspace, such an approach can never generate lasting solutions. Government, businesses and civil society should work together to develop and govern the internet according to a multi-stakeholder model, in which each focuses on their own role:

- interconnectivity is mainly a matter for the tech community;
- cyber security should be a shared interest wherever possible;
- and national security is principally a task for government.

All our efforts should proceed from the same starting point, namely that the internet must be free, open and secure.

It's instructive to make a comparison with other sectors. Take the banking sector or civil aviation. We invest in safety and we expect everyone to contribute: not just governments but also the banks themselves. Not just the airlines or the airports, but also the passengers. We do this not to curb use of these services, but rather to promote it. We invest in security for the benefit of law-abiding users, and to make criminals think twice before robbing a bank or hijacking a plane. We set standards and reporting obligations not to hamper business, but to promote a stable and reliable business environment. Security is not just the flip side of the coin, it is the coin itself. We need it in order to pay and to be paid. We need it to keep the banking system, air travel and – by extension – the internet alive.

Peace and justice cannot truly exist in a world that is unequal. One fundamental problem with the social contract underpinning cyberspace these days is that there are still too many people in the world that do not enjoy its benefits. The gap between those who are connected, and those who are not, is growing by the day. And once you are a part of cyberspace, it's becoming an ever more complex task to maintain safe and secure connections.

We need to tackle this digital divide and its consequences. That is why my country wants to invest in capacity-building in developing countries, helping them to keep the internet open and free. Training them to protect online privacy, prevent cyber crime and safeguard sensitive systems. There is much we can learn from each other. That's why we are launching the Global Forum on Cyber Expertise this afternoon.

Peace and justice cannot truly exist in a world that does not acknowledge the special status of the core infrastructure of the internet. It should be treated as a public commons, open to all, free from domination. This is the way we treat the high seas, in line with the writings of the Dutch jurist and philosopher Hugo Grotius in the early 17th century.

But that doesn't mean it should be unregulated. After all, we have treaties and practices regulating our behaviour on the high seas. And it certainly doesn't mean that cyberspace is a lawless environment, in which Hobbes's state of nature prevails. The rules and norms that apply offline, including the tenets of international law, most certainly apply online. So countries should be able to count on other states not interfering with or harming their root servers and their critical infrastructure and services.

Again, this cannot be taken for granted. We are living in a complex security environment, both physically and virtually. In the hybrid warfare that we face today, all kinds of distinctions are blurred. Conventional warfare, irregular warfare and cyber warfare merge together. Regular military forces are faced with guerrilla groups, terrorists and outright criminals. In

such an environment it's difficult to tell friend from foe, ally from enemy.

The same holds true in cyberspace. It's clear that cyber attacks can form a threat to international peace and stability. Brazen attacks on, say, a country's government websites can trigger disastrous chain reactions – especially if they can be traced back to hackers controlled by foreign governments. We need to set up a system of confidence-building measures that can help prevent destabilisation and help ensure confidence in cyberspace worldwide. Transparency about how governments operate in cyberspace will foster détente and reduce mistrust on all sides. The focus session on International Peace and Security will look at this issue in more depth, and I salute the work of the UN Group of Governmental Experts in this respect.

Your Excellencies, ladies and gentlemen,

To help bring about a free, open and secure internet in this city of peace and justice, the Netherlands – in close cooperation with its partners – is proposing an ambitious agenda for the near future. In terms of peace, this entails:

- formulating clear rules and norms for the behaviour of states in cyberspace;
- fostering greater transparency and taking confidence-building measures;
- defining those parts of cyberspace that are inviolable.

And in terms of justice, it means:

- bridging the digital divide by building capacity;
- promoting freedom and protecting privacy online;
- and to that end, setting up a regime for export controls on internet surveillance equipment.

To achieve these goals, the international community must continue to engage with all stakeholders. We need to keep cyberspace on the agenda of all relevant regional and international organisations. Action on these points will not only promote the vision of a free, open and secure internet. It will make it a reality.

Confidence in a free, open and secure internet will be a key success factor in tomorrow's world. We need to step up our efforts to realise this vision. I am convinced that the Hague Global Conference on CyberSpace will help us do so, and make cyberspace safe for the sake of peace and justice.

Thank you.

Source: *Government of the Netherlands*, April 16, 2015

Remarks by Jeh Johnson, US Secretary of Homeland Security, at the RSA Conference 2015

San Francisco – April 21, 2015

Cybersecurity is a major priority for my boss President Obama. It is a major priority for his entire Administration. It is a top priority for the Department of Homeland Security. For me personally, as Secretary, advancing my Department's cybersecurity capability is one of my top goals in office.

The Department of Homeland Security was formed in 2002, in the wake of 9/11. Counterterrorism is our cornerstone mission. But, the reality is that in 2015, cybersecurity has become a mission of equal importance.

My message to you today is this: government does not have all the answers or all the talent. Cybersecurity must be a partnership between government and the private sector. We need each other, and we must work together. There are things government can do for you, and there are things we need you to do for us.

The Department of Homeland Security is the U.S. government's central interface with the private sector in responding to and mitigating cyber threats. We are also responsible for the security of the federal civilian .gov world.

Central to our efforts is our National Cybersecurity and Communications Integration Center, or the "NCCIC."

The NCCIC is a busy place.

Almost continually, an NCCIC team is in the field, making what is in effect a house call on a company to assess a significant cyber incident and helping them fix it. For certain diagnoses, we bring in more doctors, from the NSA, the FBI, or other agencies, to assist.

The NCCIC identifies numerous vulnerabilities. Last year, across dozens and dozens of departments and agencies of the U.S. government, we identified 265 instances of the Heartbleed vulnerability, and in a three-week period reduced them to two. Last year we helped the private and government sectors address Shellshock, BlackEnergy, Havex, BackOff Point of Sale, Lenovo SuperFish, and other vulnerabilities.

We are realigning reporting relationships so that the NCCIC director has a direct reporting and information sharing line to me, the Secretary. This is the importance I place on the NCCIC in our cybersecurity mission.

We are enabling the NCCIC to provide near real-time automated information sharing to the private sector. I have directed our team to go full throttle on this. As you know, cybersecurity is about speed.

Last week the NCCIC deployed the capability to automate publication of cyber threat indicators in a machine-readable format. We reached this major milestone five weeks ahead of deadline. Today we are sharing indicators with an initial set of companies and are in the process of adding others.

Later this year, we will be in a position to begin to accept cyber threat indicators from the private sector in automated near real-time format.

We have set up the NCCIC as your primary pathway to provide cyber threat indicators to the U.S. government. Yes, the government is trying to make it easy for you.

Congress is poised to help us in cybersecurity.

Late last year Congress passed the National Cybersecurity Protection Act, which codifies into law that the NCCIC is the federal civilian interface with the private sector for cybersecurity. Late last year, Congress also passed legislation to help DHS hire and pay a highly-skilled cybersecurity workforce.

We want to go further. In January President Obama came to the NCCIC and announced that his Administration supports additional laws to establish the NCCIC as the primary portal through which the private sector should pass cyber threat indicators.

To encourage the private sector to share cyber threat indicators with the NCCIC, the President also announced that we now support legislation that will provide protection from civil and criminal liability to those who share cyber threat indicators with the NCCIC.

President Obama has proposed and supports a national data breach reporting system, in lieu of the existing patchwork of state laws on the subject. He has proposed and supports enhanced criminal penalties for cybercrime.

But, we are not just waiting for Congress to legislate.

The President has been active in issuing a number of executive orders and actions to strengthen cybersecurity.

In February 2013, the President signed an Executive Order to promote information sharing and cybersecurity best practices, by the creation of the Department of Commerce's "Cybersecurity Framework" and the Department of Homeland Security's C^3 voluntary program.

In February 2015, the President signed an Executive Order directing the Secretary of Homeland Security – that's me – to encourage the further development of private Information Sharing and Analysis Organizations, or "ISAOs."

In February the President also directed the creation of a Cyber Threat Intelligence Integration Center to be a national intelligence center that "connects the dots" related to foreign cyber threats.

Just a few days ago President Obama signed an Executive Order which authorizes the Secretary of Treasury to impose financial sanctions on those who engage in malicious cyber-enabled activities that are a threat to national security, foreign policy, economic health, or the financial stability of our country.

Two weeks ago I was in Beijing and met with the Minister of Public Security and the Minister of Cyberspace Administration of the People's Republic of China. Though we have sharp differences with the Chinese Government, particularly when it comes to the theft of confidential business information and proprietary technology through cyber intrusions, we and the Chinese recognize the need to make progress on a range of cyber-related issues. As the two largest economies in the world, the U.S. and China have a vested interest in working together to address shared cyber threats, and making progress on our differences.

We have therefore agreed to further cybersecurity discussions. I believe this will allow us to make progress on cybercrime and other shared threats.

The Department of Homeland Security also has a major law enforcement role in cybersecurity.

The Secret Service is known for the protection of our nation's leaders. The Secret Service is actually a law enforcement agency, originally formed by Abraham Lincoln in 1865 to investigate bank crime. This mission has evolved over the years to include the investigation of cybercrime.

In February of this year the Secret Service was the lead investigative agency responsible for bringing to justice one of America's most wanted cybercriminal suspects, Vladimir Drinkman.

Homeland Security Investigations is also involved in hunting down cybercrime.

The United States Coast Guard is involved in cybersecurity – by working to protect our maritime transportation system – a system that contributes $650 billion annually to the Nation's gross domestic product and sustains more than 13 million jobs – from cyber related threats.

These are some of the things your government is doing in cybersecurity.

Now, there are several things I ask you to think about.

First, we are all only as strong as our weakest link. You know this, as well as I do. The most sophisticated companies and government agencies with the best cybersecurity remain vulnerable to the most basic act of spear-phishing, if just one of our employees opens just one wrong email or attachment.

The same is true of companies with whom you do business and are linked with on the internet. There are wide differences in the level of sophistication in American business when it comes to cybersecurity. Yet we are all increasingly interconnected. This is why I am glad to see on the program for this RSA conference a session on "Combating Cyber Risk in the Supply Chain."

Those of us at this conference must leave here and encourage others to practice good "cyber hygiene."

Second, I want you to know that, when it comes to the government's cybersecurity responsibility, I am determined to root out any turf battles between government agencies. I am encouraging my people within Homeland Security to work in a cooperative and selfless fashion with our interagency partners at the FBI, NSA, Defense, Treasury, Justice and Commerce.

Now, finally, I have an ask: for your indulgence and your understanding on the subject of encryption.

The Department of Homeland Security has both the cybersecurity mission and a law enforcement/counterterrorism mission for the American people. We have feet in both camps. I

therefore believe I have a good perspective on this issue.

The current course we are on, toward deeper and deeper encryption in response to the demands of the marketplace, is one that presents real challenges for those in law enforcement and national security.

Let me be clear: I understand the importance of what encryption brings to privacy. But, imagine the problems if, well after the advent of the telephone, the warrant authority of the government to investigate crime had extended only to the U.S. mail.

Our inability to access encrypted information poses public safety challenges.

In fact, encryption is making it harder for your government to find criminal activity, and potential terrorist activity.

We in government know that a solution to this dilemma must take full account of the privacy rights and expectations of the American public, the state of the technology, and the cybersecurity of American businesses.

We need your help to find the solution.

Homeland security itself is a balance – a balance between the basic, physical security of the American people and the liberties and freedoms we cherish as Americans.

In the name of homeland security, we can build more walls, erect more screening devices, interrogate more people, and make everybody suspicious of each other, but we should not do this at the cost of who we are as a nation of people who cherish privacy and freedom to travel, celebrate our diversity, and who are not afraid.

In the final analysis, these are the things that constitute our greatest homeland security.

Thank you for listening to me.

This speech has been edited for length.

Source: *US Department of Homeland Security*, April 21, 2015