CYFY
THE INDIA CONFERENCE ON CYBER SECURITY AND CYBER GOVERNANCE

OBSERVER RESEARCH FOUNDATION

ORF CYBER MONITOR

CYFY 2014 16th & 17th October

VOLUME II | ISSUE 7 | July 2014 | www.cyfy.org

COMMENTARY

Modi's government should double down ....

Rajan Narang and Pat Cheetham

The need for improved technology is most readily apparent in the electronics sector. In 2015, India will consume an estimated $94 billion worth of electronics, a figure that is projected to grow to $400 billion by 2020.

Perils of Diffidence

Kamlesh Bajaj

India is largely on the margins of all the global debates on internet governance, surveillance and espionage. It has never sought its rightful place commensurate with its status as an IT country that is the global hub of outsourcing.

MEDIA WATCH

Cyber Security

New export control law could threaten India's cyber security

Cybersecurity Boosted After Snowden NSA Revelations

Microsoft to Open Cybersecurity Accelerator in Israel

Cyber security centre established in Dubai

Indian Banking System third most at risk with online malware

Africa Moves Towards a Common Cyber Security Legal Framework

Cyber Governance

France lashes out at internet naming body ICANN

India's only cyber appellate tribunal defunct since 2011

Kenya Internet Governance Forum (IGF) Set for July 3 in Nairobi

'Double 7' strategy may give China more control over internet: Duowei

Google and Facebook can be legally intercepted, says UK spy boss

Google search results may indicate 'right to be forgotten' censorship

IN FOCUS

ICANN 50, London, June 22-26

Analysis

Statements

Reports

ESSENTIAL READING

Commentaries

Journal Articles

Reports

EDITORIAL

COMMENTARY I

Modi government should double advanced electronics manufacturing

Rajan Narang and Pat Cheetham

On June 14, Prime Minister Modi called for increased domestic investment in the sector of science and technology. In that speech, he remarked that, "we need to give immense importance to latest technology. This will help the nation. Why should we import defense equipment? We must be self-sufficient." Modi's emphasis of a long-held national ambition reflects a desire on the part of the government to upgrade its technological capabilities to match its economic and security requirements. This outcome will not be easy or quick, but it is nonetheless a necessary one.

Technological innovation in India has historically been sluggish, in part because of low spending on research and development (R&D). India's gross domestic expenditure on R&D, or GERD, is estimated to be $44 billion dollars in 2014. This represents just 0.85% of gross domestic product (GDP). While India is the 8th largest spender on R&D in the world, its ratio of spending to GDP ranks just 32nd – well behind the Western world, as well as similarly developing countries such as China, Russia, Brazil, and South Africa. This persistent gap bodes poorly for the science and technology sector in the short term, particularly in light of India's rapidly increasing need for high-technology products.

The need for improved technology is most readily apparent in the electronics sector. In 2015, India will consume an estimated $94 billion worth of electronics, a figure that is projected to grow to $400 billion by 2020. That demand is driven by high-end electronics such as microelectronics – the nation consumes $7 billion worth of semiconductor products today, and is projected to reach $55 billion by 2020. Unfortunately, these electronics are not built in India. 65% of Indian electronics are imported, with the import-export gap projected to reach an astronomical $296 billion by 2020 – larger than any other economic sector. In short, forecasts project that the nation's paltry domestic supply will be increasingly unable to keep up with skyrocketing demand.

In recent years, policymakers have realized that the import-reliant status quo jeopardizes both the nation's fiscal health and its national security. Notably, the Singh government banned imports of Chinese telecommunications equipment in 2010 on national security grounds. Reportedly, the Huawei company later hacked into state-owned telecom infrastructure. As a result of these concerns, India has begun to prioritize the domestic development and manufacture of certain critical components such as semiconductors and other microelectronics. The 2012 National Policy on Electronics states that "Electronic system design manufacturing (ESDM) is of strategic importance. Not only in internal security and defense, the pervasive deployment of electronics in civilian domains such as telecom, power, railways, civil aviation, etc. can have serious consequences of disruption of service… We cannot be totally dependent on imported electronic components and products for such a sector." The policy also enumerated significant incentive programs to attract private investment into ESDM.

This goal of increased domestic production will be difficult for India to achieve quickly. At present, the nation does not have any domestic production of semiconductors and other advanced microelectronics. A recent East-West Center report by Dieter Ernst furthermore warns that, "historical strategies… of 'high-volume, low-cost' expansion are ending." Nonetheless, the picture is not universally grim. The report cites Indian expertise in chip design as a strong intellectual foundation for the creation of advanced chips, and thus suggests that Indian businesses pursue a strategy of 'low-volume, high-cost' production of highly advanced chips. Over the long term, more production in high-end chips will be good for the Indian market.

This is where the Modi government has an opportunity to actively influence the course of development. Despite significant delays after the implementation of the 2012 National Policy, the Singh government announced late last year that approval had been given for the construction of two semiconductor fabrication plants in Delhi and Gujarat. In two years, these fabs will go online. Their facilities will produce chips down to a size of 22 nanometers, which trail the new cutting-edge 14-nanometer Intel chips, but nonetheless are still competitive on the global stage.

Even these significant capabilities will not singlehandedly create sufficient domestic ESDM. It is both economically and strategically necessary for the government to build on the work of the last government in this sector and to ensure that its plans are implemented. In the words of geopolitical strategist Rajeswari Rajagopalan, "the previous government initiated some good policies but did not follow through on their execution;" in a similar vein, one industry leader commented to the East-West Center that "the government supported policies are non-existent, so I would not call them enablers." This lack of focus stunted advancement and has left the Modi government with a great deal of catching up to do across multiple sectors. Nonetheless, as the stark figures above show, India cannot afford to forego investment into cutting-edge science and technology any longer. Instead, Modi's government needs to double down on ESDM by successfully executing the two new fabs and looking to build two more in the near term. Economic and strategic imperatives are driving India to produce advanced electronics that can compete on the global stage, and the consequences for failure may be severe.

Rajan Narang an Account Executive at Gumbinner & Davies Communications and Patrick Cheetham is a Fellow in the Center for Revolutionary Scientific Thought in the Potomac Institute for Policy Studies.

Perils of Diffidence

Kamlesh Bajaj

Cyberspace has emerged as a global commons. It requires safe navigation by countries for trade, commerce and communication. Militaries consider it as the fifth domain — after land, sea, air and space. The internet economy, meanwhile, is growing significantly in all countries, leading to job creation, involving youth in all spheres of human activity. Nations want the internet to continue to innovate and grow; develop new business models, connect the globe through social media, create communities and remain a powerful means of communications and new ideas. However, the very same standard protocols of the internet that make it easy to connect in borderless space are used by criminals to attack private and public infrastructure as well as strategic resources. As a result, cyber crimes, espionage and cyber weapons are also on the rise. Crime syndicates, non-state actors and others continue to disrupt the peaceful uses of cyberspace. Unique characteristics of the internet, namely offence dominance, difficulty in attribution of attacks, development of cyber weapons by states and use of non-state actors to camouflage their actions are making cyberspace more and more insecure. Moreover, the applicability of international laws is not known, since the act of war by a state is difficult to establish — when started, whether ended.

Nations are developing offensive capabilities even as they preach its use for economic growth. Cases of cyber espionage, surveillance in the name of counterterrorism, and cyber warfare are high on the agenda of international discussions in an effort to ensure that the internet or cyberspace is used for the global good. The reecent stand-off between the US and China on espionage by the latter and political espionage by the former in the name of counterterrorism has escalated to high decibels. In addition, internet governance, largely under US government oversight, is another sore point in the global discussions.

India's dependence on technology as a nation is increasing — the Indian economy is going the e-way. Growth in e-commerce, e-payments, card circulation, domestic IT market spending and internet user base are the leading indicators. The government is relying on technology to solve governance problems and socio-economic problems. Technology is becoming the lifeline of critical infrastructures such as energy, telecommunication, banking, stock exchanges, etc. Businesses are leveraging technology to transform their business models. Defence and police agencies are making strategic use of technology to modernise. As a nation, we are as much the victim of cyber attacks as any other country. The attackers are local and global — driven by motives such as financial fraud or terrorism; crime syndicates; nation-states attacking directly or using non-state actors for economic and political espionage. Attacks on critical infrastructure can have crippling effects on civilians, with outcomes similar to those achieved by traditional war. Clearly, cyber security is linked to national security.

India is largely on the margins of all the global debates on internet governance, surveillance and espionage. It has never sought its rightful place commensurate with its status as an IT country that is the global hub of outsourcing. Multiple government departments have protected their turf without coming to any consensus on how to view internet governance. The involvement of the private sector in so-called public-private partnerships needs to be considerably enhanced. Cyberspace has to be managed through information-age mechanisms of cooperation and information-sharing, while India remains rooted in silos of feudal governance, which are not even based on the efficiency of industrial governance. The new government, under the leadership of Prime Minister Narendra Modi, may like to consider the following policy agenda in earnest.

One, recognising cyber security as a strategic domain of national security: there is a need to implement a robust national cyber security framework that is capable of addressing the needs of different strategic sectors, including defence. The framework implementation should be driven by a national cyber security structure that clearly defines roles and responsibilities of stakeholders and establishes coordination and collaboration mechanisms between agencies. The cyber security policies, plans and initiatives should be action-oriented, time-bound and with clearly set out responsibilities and accountability.

Two, strengthening the protection of Critical Information Infrastructure (CII) through public-private partnerships: since the CII is owned, in large part, by the private sector, its involvement in cyber security is essential. The government should launch public-private partnership programmes to protect the CII, including government and defence infrastructure. The government needs to incentivise the private sector to invest in security beyond what is required by businesses through appropriate instruments. The policies for CII protection and cyber security in general should be predictable, pragmatic, business-friendly, and forward-leaning — respecting technology advancements instead of being regressive.

Three, promoting research and development, innovation, investments and entrepreneurship in cyber security to establish India as a global hub for cyber security products, solutions and services: this entails creation of a conducive environment. Incentives should be provided for R&D in the private sector, including funding, and the issues regarding commercialisation of new products should be addressed. The government should include the cyber security sector in its international trade missions.

Four, focusing on building capabilities and skills: in defence (cyber warfare, cyber command, offensive and defensive capabilities), law enforcement agencies and judiciary (cyber crime investigation, cyber forensics), standards and workforce development, the foreign service (cyber diplomacy and negotiations), government departments (securing government assets), testing ICT products and the private sector (securing business assets, providing services to domestic and global markets).

Five, contributing to, and taking leadership of, global forums to protect India's strategic interests: as cyber security is a global issue, the international community is continuously engaged through various forums, such as the UN, Internet Governance Forum, etc, to discuss issues such as internet governance, cyber crimes, cyber warfare, security standards, supply chain risks, information sharing, and surveillance, to devise solutions. At present, India's participation in such forums is not commensurate with its cyber economy. The government should create necessary structures within the country to understand complex issues, engage in consultations with stakeholders and develop the country's position on such issues.

The writer is CEO, Data Security Council of India, a NASSCOM initiative. He was the founder director of CERT-In, Government of India.

Source: *The Indian Express*, June 20, 2014

In Focus– ICANN 50, London, June 22-26

ANALYSIS

Clarity Emerging on IANA Transition

There were three big issues at the London ICANN meeting. The most important was the globalization of IANA; the second was the release of the Expert Working Group (EWG) report on Whois, privacy and future directory services. The least important, but equally contentious was the French revolt over geographical indicator protection in the .WINE/.VIN domain. This article focuses on the critical IANA transition issue; the others will be addressed later.

ICANN's London meeting took some small but important steps forward in the IANA transition process. This happened despite some early expressions of mutual mistrust by key parties. Some of that mistrust was based on a misunderstanding, one that is beginning to be cleared up. More specifically, there was real progress in arriving at a common understanding of the relationship between the IANA transition process and ICANN's broader "Enhancing Accountability" process. Despite this progress, a new area of ambiguity and contention was identified: the role of the ICANN board in approving or intervening in the work of the IANA transition coordinating committee.

More about that at the end.

It is now clear there are two distinct kinds of accountability problems in play, and many people are conflating them. One is the accountability of ICANN's policy making process for domain names. It concerns matters such as: How can we ensure that the policy decisions made by ICANN's board are accountable to the broader community of Internet users and suppliers? What kind of appeals mechanisms or redress should there be when ICANN's policy making deviates from the correct path?

The other accountability issue relates specifically to IANA and the end of U.S. government oversight. It involves question such as: How can we ensure that ICANN's policy development is kept separate and distinct from IANA's operational implementation of changes in the DNS root zone? In other words, how can we be sure that whoever is in control of the root does not abuse that authority by implementing changes that are not first developed and authorized by the community? Also, how can we be sure that the IANA functions are performed securely, efficiently and accurately, that the 'customers' of IANA have some redress if the services are not performed properly? The end of the NTIA contract would mean that there is no longer any party with the authority to enforce these concerns; something has to replace it.

Call these Accountability type A (policy process) and type B (IANA implementation). Up to now, the term "accountability" has conflated both of those meanings. That confusion partly explains why ICANN's CEO and staff were so worried about keeping the accountability process separate from the IANA transition, and why they resisted efforts to make accountability improvements a "prerequisite" for the IANA transition. Their fear, in a nutshell, was that complex debates over the massive reorganizations required to make ICANN's policy making processes and organs fully accountable would set the bar for the transition so high that it might never happen. But that conflation also explains why other parts of the community, ourselves included, insisted that accountability was indeed a *prerequisite* for the IANA transition, and why we were extremely suspicious of ICANN management's attempt to keep accountability and IANA on separate tracks. One cannot give ICANN unchecked control of the DNS root, a critical resource for the global Internet, without some form of accountability that fills the gap left by the end of the NTIA contract. And the sad truth is that withholding control of the IANA from ICANN until it reforms is the best – possibly the only – leverage we have to effect reforms.

Our initial paper on how to globalize IANA recognized the distinction between type A and type B accountability, and now people are beginning to appreciate it. We pointed out in March that structural separation of ICANN as policy maker from IANA as implementer would prevent concentration of unchecked power in ICANN's hands and help keep IANA accountable – without having to solve all of ICANN's other accountability problems at once. Once

the two were separated, the ICANN community could take a longer-term, less rushed approach to reforming ICANN's policy making processes. Issues such as the role of members in electing the board, ICANN's legal status, new appeals mechanisms and the like could take years to develop and implement. It is unwise to tie the IANA transition to those changes.

At a meeting with the Non commercial Users Constituency in London, NTIA director Lawrence Strickling and State Department Ambassador Danny Sepulveda confirmed our sense that structural separation of IANA from ICANN is not 'out of scope.' While the IANA transition and accountability are separate, with the accountability track dealing with higher level governance questions, they have no problem with an IANA transition plan that tries to align DNS governance with the governance of protocol paramters and numbers, where policy making and IANA implementation are conducted by separate organizations. The IANA transition Coordinating Committee, Strickling said, "can do what it wants" in that regard. Strickling himself expressed support for separation of policy and implementation.

The role of the coordinating committee for the IANA transition (CC-IANA) is now becoming the next interesting issue. Fortunately, the committee is no longer viewed as a steering committee that makes the plan for the IANA transition, but more as a coordinator of the three distinct communities with a stake in the transition – names (ICANN), numbers (RIRs) and protocol parameters (IETF). The GAC, true to its status as the voice of dinosaurs in the Internet ecosystem, wants to be given 5 seats on the CC-IANA. Apparently it is viewing the CC-IANA as a voting body, and believes that governments cannot be "represented" by other governments. But the purpose of the GAC seats on the CC-IANA is not to vote or to "represent" all diverse views, but to serve as a liaison to the governments. The CC-IANA is already overly-large, and tossing an additional 3 people on to it simply to assuage unintelligent political calculations should not happen. GAC's demand should be rebuffed; or, at the very least, the CC-IANA should meet in its current form and deliberate on whether to add additional seats for governments.

A very constructive session, moderated by technical community stalwarts Patrik Faltstrom and Jari Arkko, introduced the ICANN London meeting to the issues and problems that need to be addressed by the CC-IANA. Still, the idea that "the community decides" what happens is not an entirely satisfactory or workable understanding of the situation; the CC-IANA must take community input and assemble it into a package, a proposal, and decide when the proposal meets the demonstrated concerns of the three different communities. It then needs to transmit the proposal to the NTIA for approval. Unfortunately, there seems to be no clear understanding of that process at the moment.

The public comments on the IANA transition should have conveyed a clear message to ICANN that its board must not be in a position to vet, modify or approve the outcome of the CC-IANA process. ICANN's board is an interested party in the outcome of the IANA transition. Its organizational self-interest leads it to prefer some kind of proposals over others. The idea that the ICANN board would be able to change or veto proposals that are broadly acceptable to the community as a whole contradicts the NTIA's mandate that ICANN is to convene, not control, the process.

Source: *Internet Governance Project*, June 28, 2014

Web Naming Group Pushes Ahead on Governance Transition

ICANN Oversight Preparing to Move to New Model

The battle for power over control of Web addresses is heating up as domain names including .com, .org and even .london are losing prominence as traffic funnels through mobile apps, search engines and social networks, Internet experts say.

But representatives from businesses, nonprofit organizations and governments who met in London on Monday for the largest-ever meeting of the organization that makes decisions about the names and numbers that make up the Internet's architecture said domain names still serve a core function: proving authenticity.

"If I asked my children [when] is the last time you typed a domain name, they probably wouldn't remember," said Fadi Chehadé, president and chief executive officer of Internet Corporation for Assigned Names and Numbers, or Icann.

Still, he said, a domain name can assure people that they are visiting an authentic site, helping to prevent fraud or counterfeit websites.

The oversight of Icann is slated to pass by late 2015 from the U.S., which had long controlled the Los Angeles-based nonprofit, to a new, international group that has yet to be formed. Icann has said it would form a committee to come up with a new governance model palatable to the U.S.

The U.S. has long said it intended to give up control, and the move has been particularly welcomed outside the U.S. after government-led spying programs were revealed by former National Security Agency contractor Edward Snowden.

On Monday, government appointees attending the meeting—one of three annual conventions—said they worried the transition would happen too fast or that the decision-making might not include all views.
The importance of the body was illustrated this week when wine producers pushed back against the planned .vin and .wine domain names, saying they believe the names could confuse consumers into buying inferior wines.

Mr. Chehadé said the wine producers had a valid concern, but they should go through the normal channels of Icann to be heard. He said it showed how important domain names still are for authentication purposes.

In addition, businesses still want control over domain names for branding purposes. "I may care if I'm putting it in my advertising," said J. Scott Evans, an associate general counsel who works on trademarks and other areas for Adobe Systems Inc. ADBE +0.90%
The london domain name, which became available in April, has started to attract luxury goods retailers who want to attach the cachet of the London city brand to their products, said Jean-Louis Bravard, who is in charge of the .london domain name. "We are seeing London brands perceiving [the domain] as an extension of their brand, he said. He declined to name the retailers.

The meeting, which continues through Thursday at the London Hilton Metropole, attracted more than 3,300 registrants.

Source: *The Wall Street Journal*, June 23, 2014

STATEMENTS

ICANN"s Generic Names Supporting Organization (GNSO) – The statement was read aloud during a June 26th session on the IANA transition process held on the last day of the ICANN 50 public meeting in London.

The entire GNSO join together today calling for the Board to support community creation of an independent accountability mechanism that provides meaningful review and adequate redress for those harmed by ICANN action or inaction in contravention of an agreed upon compact with the community. This deserves the Board's serious consideration - not only does it reflect an unprecedented level of consensus across the entire ICANN community, it is a necessary and integral element of the IANA transition.

True accountability does not mean ICANN is only accountable to itself, or to some vague definition of "the world," nor does it mean that governments should have the ultimate say over community policy subject to the rule of law. Rather, the Board's decisions must be open to challenge and the Board cannot be in a position of reviewing and certifying its own decisions. We need an independent accountability structure that holds the ICANN Board, Staff, and various stakeholder groups accountable under ICANN's governing documents, serves as an ultimate review of Board/Staff decisions, and through the creation of precedent, creates prospective guidance for the board, the staff, and the entire community.

As part of the IANA transition, the multi-stakeholder community has the opportunity and responsibility to

propose meaningful accountability structures that go beyond just the IANA-specific accountability issues. We are committed to coming together and developing recommendations for creation of these mechanisms. We ask the ICANN Board and Staff to fulfill their obligations and support this community driven, multi-stakeholder initiative.

Ed Vaizey (UK Communications Minister) speech at the ICANN 50 opening ceremony

London – June 22, 2014

Good morning everyone. Welcome to the UK, welcome to London and welcome ICANN 50.

It's hard to believe that in the 15 years since ICANN first met in Singapore, this event has never taken place in the UK. Britain is a world leader in digital technology. The internet economy is already responsible for more than eight per cent of UK GDP – that's a greater share than in any other G20 country.
Much of this success is down to the innovative spirit of British technology pioneers. But Government has also played its part. We're on track to deliver superfast broadband to 95 per cent of the country by 2017, giving hi-tech and traditional businesses the infrastructure they need to access global markets. We've created tax relief of up to 225 per cent for research and development.

The government is leading by example – we're aiming to make all government services digital by default. You can already go online to apply for everything from a driving licence to permission for burial at sea!

It all helps to explain why the UK is the highest-ranked G20 country in the Global Innovation Index.
But it's not the only reason why it's fitting that ICANN's 50th meeting is taking place in London. About 10 miles to the South West of where we are today lies the childhood home of Tim Berners Lee, the Great British brain behind the creation, a quarter of a century ago, of the world wide web.
Head about 10 miles to East and you'll find the Olympic Stadium, where Sir Tim memorably tweeted to the world during the 2012 Opening Ceremony. His message – "This is for everyone" – was a fitting description not just of the Games, but also of the web and the internet. And, just as importantly for today's discussion, for how the UK believes the internet should be governed.

The system of governance we have in place now has by any measure been successful in creating the opportunity for economic growth and intellectual freedom. That includes ICANN of course in the performance of its role in coordinating and developing the domain name system so that it serves the global community. The current review of ICANN accountability is an important step therefore.

And that links to the IANA function which has performed so well under the existing arrangements under contract to the US government that the average Internet user might well wonder what we are talking about. We often talk about the "stewardship" of the IANA function, and I always think it's the perfect way of describing the role. It's not about regulation or ownership. It's not about one country controlling the internet or dictating its terms. It's about nurturing it, supporting it, creating the environment in which it can develop and grow so that it can safely be handed on to the next generation.

But the internet is constantly evolving and the way it is stewarded has to evolve too. That's why the UK government strongly supports the moves by the US to "let go" of the IANA function. It's a huge step forward in making this global resource a truly global enterprise. And it's a move that has a symbolic mirror in the very make-up of ICANN, which has shifted from being a US-based and US-dominated organisation to one that is seen as much more international.

Of course, with such a vital role to play, it's absolutely imperative that the alternative model we move to is maintains the security, stability and resilience that underpins the global domain name system. That it's capable not just of doing the job as well as the old way, but of doing it better. And, above all, that it's capable of adapting and coping with the next wave of internet-enabled devices, the so-called internet of things. That is why as we engage with this final phase of privatisation of the domain name system, we must be

cautious and not rush to change the current arrangements.

This is only going to happen if the system continues to evolve and develop organically with the full involvement and input of all interested parties worldwide. And that can only happen if the act of stewardship continues to be carried out in a collaborative, bottom-up way. In a spirit of global co-operation rather than state-centred regulation.

Some say this can't work, that such a monumental task can only be undertaken at a governmental or supranational level. But look at how well the ICANN model has worked so far. In less than 20 years the internet has revolutionised the way the world works, talks and studies. And this explosive growth wasn't managed by governments, it was driven by you.

Just look at the principles that were agreed at the Global Multistakeholder Meeting on The Future of Internet Governance – NETMundial. They weren't created by politicians, or by the UN or by anonymous men in shadowy rooms. They were created in the open by the community that supports and curates the internet, the people without whom life online would be simply impossible. The people who have the best possible grasp of both the challenges facing the internet and the means required to tackle them. Or to put it another way: the people in this room.

The principles developed at NETMundial are as robust as they are simple. Internet governance should be built on a fully inclusive, multi-stakeholder process, ensuring the meaningful and accountable participation of everyone involved. Decisions should be made in a bottom-up, open, participative, consensus-driven way. There should be a suitable level of accountability, with mechanisms for checks and balances as well as for review and redress. Anyone affected by an internet governance process should be able to participate in that process.

I'm proud to say that the UK government wholeheartedly supports these principles as a basis for the global internet governance framework.

Again, I know that some don't share this view. But what is the alternative? Top-down, centralised decision-making. A bureaucratic world-wide web of red tape. The internet being run not by the people who make it work on a daily basis but by horse-trading politicians behind closed doors.

Just imagine an internet that relied on governments agreeing on things! Internet governance has to match the rapid pace of change experienced by the internet itself. But let's face it, "Rapid change" and "inter-governmental agreement" are not concepts that generally go well together.

That is why I was so keen to host a high-level meeting of governments here today. We are not here to make decisions on your behalf. We are here to talk about the ideas you have developed. We are here to learn more about ICANN, and for you to learn more about us.

So governments have a role in internet governance, just as the technical, civil and academic communities do. And we also have responsibilities.

Governments have to act proportionately in cyberspace, empowering users of the internet by promoting and safeguarding freedom of expression, cultural diversity, gender equality, information, education and skills.

We have to ensure that domestic legal frameworks are fair and consistent by ensuring transparency of legal process and accountability for government decisions and that the law applies equally online as it does offline. They have to provide equitable civil processes for dispute resolution so that citizens can enjoy due legal process and can enforce their rights.

And as we've seen in the UK, governments have to establish and promote a robust global internet infrastructure that provides equitable access for all, promotes economic development and job creation, and allows more people to enjoy a better quality of life.

What governments shouldn't be doing is attempting to manage how the internet is run. As Fadi Chehade has said, "The Internet is the Greatest Public Gift". It doesn't belong to anyone, it isn't controlled by anyone.

The internet itself has endured precisely because it is bigger than any one country.

ICANN 50 is taking place at a critical moment in discussions about the future course of internet governance. I have already referred to NETmundial meeting in Sao Paulo – the key outcomes of which will be discussed at this meeting.

The recommendations for strengthening the global Internet Governance Forum should feed directly into the 9th IGF in Istanbul in September. Following closely on from the IGF, the International Telecommunication Union – the ITU – will have the opportunity to consider its role in standards and capacity building at the Plenipotentiary Conference in Busan, South Korea, in October and November.

All these processes and linkages are against the backdrop of the WSIS+10 [Wissis plus 10] review by the UN General Assembly. The outcomes of the 2005 Tunis summit, which embedded the multi-stakeholder approach in the Internet governance eco-system, have been implemented very well. You only need to look at the highly detailed evaluations produced by UNESCO last year and the recent ITU High Level Event to see that.

So it makes sense for next year's final stage of the UN review process to also be undertaken with the active participation of representatives from all over the world.

We must explore in these fora how we can encourage alliances and active collaboration among stakeholder constituencies and sources of expertise.

A key objective must be to strengthen existing mechanisms and processes, such as the Internet Governance Forum, which we in the UK have always supported.

I hope that, in future, we will see an IGF whose outcomes are more immediate, visible and tangible, and that there will be stronger links between the main IGF and its many regional and national multi-stakeholder IGFs and with other entities in the Internet eco-system.

Achieving this will help with what has to be our number one goal – bringing the next billion people from developing countries into the global digital economy, with all the social and economic benefits that entails.

Earlier this year the World Wide Web celebrated its 25th birthday, 25 years of unparalleled expansion, economic growth and social good. ICANN is key to ensuring that this success continues for the next 25 years.

Sir Tim Berners Lee said "this is for everyone". It's up to us to make sure it stays that way.

REPORTS

"GAC communiqué", ICANN 50 London", *Governmental Advisory Committee*, June 25, 2014

"Report on ICANN 50 London, June 22-26, 2014", *Council of European National Top Level Domain Registries*, June 27, 2014

Transcripts, Presentations and Audio files of the ICANN 50 proceedings can be found here.

Cyber Security

New export control law could threaten India's cyber security programme

India has expressed concerns over an attempt by the Western countries to include cyber security technologies under the Wassenaar Arrangement, a global agreement on arms and weapons export control. Changes were made to the Wassenaar Arrangement in December 2013 at a plenary meeting held at Vienna following the Snowden revelations.

May hit Indian firms

"These changes could have severe impact on India's cyber security programme — both software and hardware — as these would come under export control regime, the entire inventory of high-end cyber technology is with the Western countries like the US and they may deny products to Indian organisation," said a senior Government official.

A high level meeting of the National Security Council was recently held to discuss the next course of action. The problem is that the products included in the control list have not yet been made public and the next round of plenary meeting to be held at the end of this month is expected to see the formal adoption of this agreement.

The 41 signatory states include the US, Russia, Japan, France and Germany. Since India is not part of the agreement, it does not have access to the decisions or means to influence the proceedings. Therefore, Indian may seek membership to the exclusive club.

The UK and French governments are leading this move to clamp down on cyber technology in a bid to address fears around cyber warfare and spying. According to foreign media reports, western intelligence agencies are concerned about such technologies falling into enemy hands.

While Indian authorities admit that the proposed export rule could have its merits, they want Western countries to take on board India's concerns with respect to access to high-end technologies for genuine security purposes. "The best way to deal with this would be to have our own technologies and invest in R&D but that would take time. We would like to engage with countries like US and UK to take our view on board before listing out products under export control," said a Government directly dealing with the issue.

Pre-emptive move

The official also said that as a pre-emptive move India was looking to purchase critical technology before the new arrangement is finalised. An expert committee has been set up to figure out the future course of action, including negotiating with six countries — the US, the UK, Israel, Germany, France and Canada.

Source: *The Hindu Business Line*, June 19, 2014

Cybercrime costs global economy up to $575 bn annually: McAfee

The growing menace of cybercrime is impacting the global economy significantly with estimated annual losses of up to $575 billion, a report by cybersecurity solutions firm McAfee revealed. The report, Net Losses — Estimating the Global Cost of Cybercrime, by Centre for Strategic and International Studies (CSIS) and sponsored by McAfee also said the cost includes the effect on hundreds of millions of people who had their personal information stolen.

"We estimate that likely annual cost to global economy from cybercrime is more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion," the report said. Parts of the losses from cybercrime are directly connected to 'recovery costs' or the digital and

electronic clean-up that must occur after an attack has taken place. Cybercrime damages trade, competitiveness, innovation, and global economic growth. Studies estimate that the Internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly, it added.

Based on CSIS estimates, cybercrime extracts between 15 per cent and 20 per cent of the value created by the Internet. Explaining the process for reaching the impact figure, the report said, "If we used the loss by high-income countries to extrapolate a global figure, this would give us a global total of $575 billion."

"Another approach would be to take the total amount for all countries where we could find open source data and use it to extrapolate global costs. This would give us a total global cost of around $375 billion." The report further said that a third approach would be to aggregate costs as a share of regional incomes to get a global total. "This would give us an estimate of $445 billion. None of these approaches are satisfactory, but until reporting and data collection improve, they provide a way to estimate the global cost of cybercrime and cyber espionage," it added.

Cybercrime costs include effect of hundreds of millions of people having their personal information stolen. Incidents in the last year include over 40 million people in the U.S., 54 million in Turkey, 20 million in Korea, 16 million in Germany and more than 20 million in China, the report revealed. "One estimate puts the total at more than 800 million individual records in 2013. This alone could cost as much as $160 billion per year," it said.

Cybercrime's effect on intellectual property (IP) is particularly damaging and countries where IP creation and IP-intensive industries are important for wealth creation lose more in trade, jobs and income from cybercrime than countries depending more on agriculture or industries of low-level manufacturing, the report found. Accordingly, high-income countries lost more as a percent of GDP than low-income countries.

Source: *The Hindu*, June 10, 2014

Cyber criminals cash in on World Cup frenzy

With the FIFA World Cup fever gripping one and all, cyber criminals have sensed an opportunity to target users online, as well as offline. Across the globe, security advisories are cautioning users about possible scams and phishing attacks. Security solutions firm Kaspersky Lab has advised football fans travelling to Brazil to use be cautious while using local AC/DC chargers, as cyber criminals are using fake AC/DC chargers to steal data from smart-phone users.

A malicious AC/DC charger will, while charging your phone's battery, steal information from your smart-phone. The interception will happen via a USB connection, as most plugs use such connections. In some cases, fake chargers also install malware capable of tracking your location and stealing notes, contacts, pictures, messages, call records, saved passwords and browser cookies.

"Cyber criminals know when people are away from home and need their smart-phones to access maps, routes and other information, they tend to use any available charger, even if it's just for a few minutes. Keep in mind you could fall victim and lose sensitive personal data," said Dmitry Bestuzhev, head of Kaspersky Lab's global research and analysis team in Latin America.

Another threat is accessing Wi-Fi. "Kaspersky Lab security experts conducted research on Wi-Fi access in São Paulo. They drove 100 km around the city and checked about 5,000 different access points popular among tourists — parks, malls, airports, etc. It turned out 26 per cent of the 5,000 open Wi-Fi networks in São Paolo didn't use encryption," the company said.

Security advisors have also cautioned those travelling to Brazil against fake and malicious versions of World Cup-themed apps. Trend Micro, a security solutions provider, has already found 375 questionable or outright malicious World Cup-themed apps. "The vast majority of these apps lurks from third-party app stores. So, users are advised to avoid them altogether or be extra careful when reviewing apps they want to install from them. Installing a mobile security solution

is also a good idea," said Dhanya Thakkar, managing director (India and Southeast Asia), Trend Micro.

World Cup fans have also been cautioned against free ticket scams, news service scams and online streaming scams. Security solutions and storage specialist Symantec has identified several email scams and expects to see attempts to target fans on social networks. "The most common scam around the World Cup involves free tickets. After all, which fan wouldn't want an all-expenses paid trip to Brazil? Scammers know a dream come true is hard to let go, and circulate emails promising everything imaginable," said a Symantec blog.

Scammers are also targeting users through their favourite players. "Currently, emails are being circulated about Neymar da Silva Santos Júnior, the young star player in the Brazilian national team. The email contains a malicious word document that exploits a known vulnerability in Microsoft Word. Interest in players such as Neymar and Argentinian Lionel Messi are used as baits to target victims, through email or social networking services," the blog said.

Source: *Business Standard*, June 27, 2014

Rights groups say UK conducts mass cyber-snooping

Britain's top counter-terrorism official says the country's espionage rules allow its electronic spy agency to routinely intercept online communications between Britons who use US-based platforms such as Facebook, Twitter and Google.

A witness statement by Office for Security and Counterterrorism chief Charles Farr, made public on June 17, said data sent on those services is classed as "external" rather than "internal" communications because the companies are based outside Britain. Britain's Home Office confirmed the document was genuine. It was written in response to a legal action by civil liberties groups who are seeking to curb cyber-spying, and was published by the groups on June 17.

Britain's electronic intelligence agency, GCHQ, has broad powers to intercept communications outside the country, but needs a warrant and suspicion of wrongdoing to monitor Britons. In the document, Farr said some internal communications are intercepted under the external rules, but they "cannot be read, looked at or listened to" except in strictly limited circumstances. He said that was a "significant distinction."

Civil liberties organisations say the rules are too vague and allow for mass surveillance. "The security services consider that they're entitled to read, listen and analyse all our communications on Facebook, Google and other US-based platforms," said James Welch, legal director of Liberty — one of the groups involved in the legal action. "If there was any remaining doubt that our snooping laws need a radical overhaul there can be no longer."

Farr said that emails sent between two people in Britain would usually be classed as internal even if they travelled by route outside the country. But Facebook and Twitter posts or Google searches that went to data centres outside the British Isles would fall under the external category. GCHQ did not immediately respond to a request for comment.

Source: *The Indian Express*, June 17, 2014

Cybersecurity boosted after Snowden NSA revelations

Silicon Valley has come a long way in boosting privacy and cybersecurity since reports in June 2013 disclosed that the National Security Agency was collecting data from Internet companies. Tech companies including Google, Twitter and Yahoo commemorated a year of news reports detailing secret government surveillance on June 5 by supporting campaigns that both pressure government privacy reform and raise consumer awareness about cybersecurity. Those three companies were among the nine firms that make up the Reform Government Surveillance advocacy group, which called for the Senate to boost privacy protections against mass surveillance with a stronger version of the USA Freedom Act bill. The House passed a version of the bill to end mass phone

surveillance that privacy advocates criticized as ineffective on privacy.

"Over the last year many of our companies have taken important steps, including strengthening the security of our services and taking action to increase transparency," the group said in a letter to the Senate. "But the government needs to do more." The separate Reset the Net advocacy campaign against mass surveillance also gives Internet and mobile cybersecurity tips, while companies including Google pledge to boost their encryption. Google also released a test version of a program to keep Gmail encrypted until it reaches other Gmail users.

"Countless organizations and companies have really stepped up their game when it comes to hardening their systems and protecting the security of our communications," Bankston says. Reports have shown the NSA requested information from Internet companies through the Foreign Intelligence Surveillance Act court, which nearly always approved a government query, but has also tapped Yahoo and Google servers, installed back doors onto routers and installed spyware onto computers. The Electronic Frontier Foundation advocacy group made a handy and lengthy list of all the disclosures that expanded public awareness of government surveillance.

"The Snowden leaks have taught tech companies a hard lesson that not only do they have to secure their services against Chinese spies and hackers, but they also need to treat their own government as a security threat," Bankston says. Despite this increase in awareness, future consequences of the Snowden leaks are uncertain for tech companies. Concerns about a perceived lack of privacy protections could damage sales of U.S. tech services abroad, boosting efforts in foreign countries to develop alternatives to U.S. tech gear and Internet services. China already offers domestic websites that support government censorship including Baidu, an alternative to Google, but some companies including Apple are also trying to gain customers among that nation's growing middle class. Concerns about the NSA have also fuelled efforts in the European Union to enact privacy rules that could make compliance expensive for U.S. tech companies and damage their business models for online advertising.

The Reform Government Surveillance group advocates that Internet companies rely on the trust of their users, and the leaks about broad NSA surveillance have damaged that trust with criticism from foreign countries. Facebook CEO Mark Zuckerberg has also said "the government blew it" by failing to be transparent about its surveillance in a way that might help international customers feel safer about using U.S.-based Web services.

When the Obama administration said it was only collecting information on people outside the United States after the news reports in June 2013, Zuckerberg has said he responded, "Oh wonderful. That's really helpful to companies who are trying to serve people around the world."

Source: *U.S. News*, June 05, 2014

Microsoft to open cybersecurity accelerator in Israel

Microsoft is to open a new cybersecurity accelerator in Israel in a bid to capitalize on the country's expertise in the field, according to a report in TechWorld. The accelerator will be a joint venture between Microsoft Ventures, the start-up arm of the tech giant, and Jerusalem Venture Partners, Israel's leading cyber security investor.

The intention is to create an environment that will help Israeli cybersecurity startups create products and services that can address some of the world's most concerning cyber security threats. Israel has already spawned several successful security companies, including Cyvera, Fortscale and Check Point.

During the first four-month program, set to run between September 2014 and December 2015, Microsoft will provide between six and eight start-ups with oversight and expertise from industry executives, as well as "free tools" and anything else they might need to help them deliver breakthroughs in cyber technology and services.

"Our accelerator program leverages the Microsoft worldwide footprint to give start-ups unparalleled routes to customers and partners," said Hanan Lavy, director of Microsoft Ventures Accelerator. "We use this power to push start-ups to their success. We are eager to work closely with JVP to provide unique opportunities for entrepreneurs in our accelerator."

JVP Cyber Labs, is an early-stage investment vehicle aimed at identifying, nurturing and building the next wave of cybersecurity companies to emerge from Israel. It has pledged to give $1 million to one start-up at the end of the accelerator program, together with a place in its own incubator located in Be'er Sheva.

"We put special emphasis on working with strategic partners, such as Microsoft, to get market validation for the significant innovations we are witnessing in the cybersecurity space," said Yoav Tzruya, partner at JVP Cyber Labs. "It is our top priority to create an ecosystem which nurtures entrepreneurs and start-ups independently of our portfolio." The program will be run out of the existing Microsoft Accelerator facility in Tel Aviv.

Source: *Haaretz*, June 04, 2014

Cyber security centre established in Dubai

A cyber security centre has been set up in Dubai to protect government information systems and the telecom network. His Highness Shaikh Mohammad Bin Rashid Al Maktoum, Vice-President and Prime Minister of the UAE, in his capacity as Ruler of Dubai, issued Law No 11 of 2014 establishing the centre. The centre aims to develop the necessary cybersecurity methods, increase the efficiency of ways of protecting information and the exchange of information among all government bodies in Dubai. Shaikh Mohammad also issued Resolution No 12 of 2014 forming the board of the centre, under the chairmanship of Mohammad Daen Al Qamzi.

The centre has been tasked with drawing up and implementing Dubai's policy for government information security, and setting criteria to ensure cyber security. It will also prepare a strategic plan to deal with any threats and cyber attacks on government information in cooperation with government bodies. All information and data provided to the centre by government bodies shall be treated as confidential information.

Government bodies and personnel are obliged to follow the cyber-related rules, regulations and criteria set by the centre. The centre will also issue permits for the import and export of encryption software and hardware and penetration testing services. The centre will be responsible for combating all forms of cyber crimes in coordination with government, regional and international authorities. It will provide technical support and consultancy services to government bodies. It will also provide services to prevent hacking telecom networks and information systems. The centre will propose legislation related to cybersecurity, increasing awareness as well as organising conferences and seminars related to the centre's functioning.

The conferences and seminars will be organised in cooperation with regional and international organisations. The centre is mandated to set the necessary rules and regulations to prevent any attempt to disrupt and sabotage telecom networks or the content of any information systems.

It is allowed to take all necessary measures to thwart any cyber attack. The centre is also tasked with contacting the National Cybersecurity Authority, and providing information and data requested by the authority to help it carry out its duties.

Source: *Gulf News*, June 11, 2014

Cyber security incidents continue to rise: ASD

The Cyber Security Operations Centre (CSOC) arm of the Australian Signals Directorate (ASD) intelligence agency responded to over a third more security incidents involving government departments last year compared to the year before, according to its 2013 report.

While the increase for 2013 wasn't as marked as the 119 percent hike recorded for the 2012 year, it was nevertheless a jump of 37 percent to 940 responses. In

total, the number of cyber security incidents went up by just over a fifth in 2013, hitting 2168.

Just under half of incident responses were at the federal government level, CSOC said, with local government making up 11 percent of callouts. The vast majority of threat adversaries were what CSOC termed "foreign state sponsored." It did not reveal which states were behind the attacks on Australian government departments.

In comparison, so-called Hacktivism through groups such as Anonymous amounted to just three percent of attacks, and organised cybercrime was behind nine percent of CSOC recorded incidents. A full two-fifths of threats were by unidentified adversaries, CSOC said. The favoured vector of attack in 2013 was social engineering via email messages. However the proportion of email-borne attacks dropped from 63 percent in 2012 to 53 percent last year.

Attackers would try to lure victims to open attachments in messages with subjects pertaining to the G20 and ASEAN group of countries, taxation, job offers and news. Microsoft Word files and ZIP compressed attachments containing malicious code were the two most popular types used by attackers, followed by Java .jar files, PDF documents and RAR archives. CSOC also spotted new attacks last year, using cloud storage providers such as Dropbox to host executable code, distributing malicious Java .jar files as attachments in emails, and messages that use real, trusted email sender addresses to trick victims.

While it recognised Java as being useful due to its portability across many operating systems and computer architectures, the security centre took a swing at Australian government agencies being slack with applying updates.

"Although each new version of Java undergoes heavy scrutiny by the IT community for new security vulnerabilities, many Australian government agencies have poor patching practices, leaving them exposed to vulnerabilities that are exploited by cyber adversaries." - CSOC

Java is seen as a growing threat to Australian government networks and several strategies to stop government users from falling victim to cyber attacks are proposed by the CSOC. These include technical measures such as hardening users applications to prevent Internet-hosted Java code from running and removing unneeded browser and PDF viewer features. Email and web content filtering is also proposed, and CSOC also suggest that workstations and servers are based on a hardened standard operating environment that disables undesired functionality such as the next generation IPv6 Internet addressing protocol, Microsoft's LANman protocol, and autorun from optical discs and detachable storage.

Source: *IT News*, June 19, 2014

Indian banking system third most at risk with online malware: Report

Banks in India have been increasingly offering the online platform to their customers for their convenience, but this has also resulted in an increase in online malware in the banking system. Japanese security firm Trend Micro, in its report on cyber crime, reveals that in the first quarter of this calendar year (January-March) India was the third most-affected country in the world by the online banking malware.

In the Jan-March quarter this year, United States led the charts with 23 percent exposure to being prone to online malware, followed by Japan at 10 percent and India at 9 percent. In the quarter before this (Oct-Dec 2013), India was at the 7th position with only 3 percent exposure to online banking malware.

"The number of online bankers in the India has improved the overall industry but has resulted in significant rise in malicious activities," said Dhanya Thakkar, Managing Director, Trend Micro (India & SEA). He adds that, "the improvements in the banking industry and the trend towards making online payments have caused such fluctuations in the growth of banking malware. Also, the introduction of new techniques by cybercriminals causes these changes. Online banking malware creators updated their portfolios yet again in Q1, 2014 with the addition of

new routines to their usual weapons of choice, and hence there was a spike in this quarter. "

The number of online banking malware detections overall has also picked up. This quarter it reached roughly 1,16,000, showing a slow but steady increase from 1,13,000 detections in the first quarter of 2013. A malware is a software designed to disrupt or damage a computer system. An earlier survey by Trend Micro had also pointed out that 15 bank related mobile apps and 39 online payment gateways, among several others, stand the risk of being exposed to cyber criminals. According to the study, social networking sites, shopping and health care apps used by Indian users are vulnerable. Apart from mobile apps, 611 websites with the .in domain in the country were also found to be vulnerable, the Trend Micro survey reveals.

Source: *Business Standard*, June 04, 2014

Africa moves towards a common cyber security legal framework

For several years, African states have been working towards common cyber security norms and regulations through the African Union (AU). From June 20-27, the AU Heads of State will meet and are expected to adopt a new Convention on Cyber Security and Personal Data Protection. While Access and other partners criticized an earlier draft of the Convention, the rewritten draft has yet to be released to the public, even as it races closer to adoption.

Background

Since 2009, the African Union (AU), has engaged in efforts to harmonize various information and communications technology (ICT) regimes, particularly around cyber security laws. Discussions about the establishment of a common framework have been ongoing since a 2009 directive, the Oliver Tambo Declaration. In 2013, a draft African Union Convention on the Confidence and Security in Cyberspace (AUCC) was made pursuant to the resolution of the Assembly of Heads of State and Government of the African Union and was published on the African Union website for the African internet community to discuss. Major concerns were voiced around this draft, and in May 2014 it was revised to a final version of the Convention, which is now set to be approved by African Heads of State at the end of June.

Delay in Passage

The AUCC was scheduled to pass during an AU meeting in January 2014, but was delayed as a result of protests from the private sector, civil society organizations, and privacy advocates, who had very little involvement in the process. Several leading voices in African internet policy spoke out against the draft Convention, including: KICTANet and ISOC-KE in Kenya, and on the I-Network list moderated by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) and ISOC - Uganda. Access also raised concerns and transmitted comments about the previous draft.

According to a presentation from the African Union, telecom/ICT experts were involved in the drafting process and discussions. However, it is unclear who these experts were, what sectors they came from, or how they were chosen.

The AUCC was supported by some government stakeholders and regional multilateral entities, but many in the internet community opposed it as the treaty contained a number of provisions that could violate user privacy, chill online expression, and endanger other rights.

On May 12 and 13, 2014, a meeting of experts from the AU members' justice ministries undertook a thorough review of the AUCC; on May 15th, it was adopted and scheduled for presentation at the 23rd African Union Summit, 20 – 27 June 2014 to be held in Malabo, Equatorial Guinea. The AUCC was adopted as the "African Union Convention on Cyber Security and Personal Data Protection."

The final outcome of the AUCC has not yet been released and Access cannot confirm whether the concerns raised with the previous draft were addressed. Without transparency, it is very difficult for civil society and other stakeholders to play a meaningful role in the drafting and political process

around this potentially far-reaching convention. Given that the previous draft raised a number of concerns from civil society, negotiating this kind of convention in the dark raises a number of human rights and legitimacy concerns. In the absence of having the final text, we thought it might be helpful to highlight the concerns that were raised with the previous version of the AUCC.

Contentious Provisions that caused delay of transmission to heads of State and Government

In short, the draft convention includes provisions on electronic commerce, personal data protection, cybercrime — with a special focus on racism, xenophobia, and child pornography — and national cybersecurity. It also encourages member states to promote cybersecurity education for information technology professionals and to add to their legal codes criminal offences for hacking computer systems. Below, we will expand on these problematic issues in the draft text.

Infringing on the right to privacy

Articles II (8); II (9); II 28(2); and II 36(9) of the draft AUCC, allow African states to process personal and sensitive data without the owner's consent for the purpose of state security and the public interest. Furthermore, the government does not have to go before a judge to get approval to violate user privacy in this way, leaving the door open for abuse.

Article I (4) of the convention compels a person or corporation engaging in electronic financial transactions (e.g M-PESA) to provide full identity information as prescribed in the clause such as his/her name, identification number, and contact information among other information. This provision puts personal information at risk, given the fact that very few African countries have comprehensive data protection laws. One does not need to look far to see the kind of abuse that can occur in this environment. Recently, a number of Kenyans were unknowingly registered with various Kenyan political parties without their consent; Safaricom, a major African telecom suggested that M-PESA agents might have sold M-PESA registration and transaction records to the political parties.

Lack of limitations on judicial power

Article III (55) provides for, "...the investigating judge [to] use appropriate technical means to gather or register in real time the data in respect of the content of specific communications in its territory, transmitted by means of a computer system..." The provision empowers judges to assume the role of the prosecutor in both common law and civil law African countries and does not provide checks and balances to ensure a separate investigation and adjudication process.

Looking forward

Already, we can see that advocacy initiatives by individuals, civil society, and academia representatives have had an impact on this process. During Africa ICT Week in December 2013, officials from the African Union Commission met with individuals, civil society, and academia representatives who were opposed to the initial draft. At the meeting, the AU Commission agreed to examine input received by concerned stakeholders and provide explanation and justification regarding areas of disagreement.

We note that this new document is named, the "African Union Convention on Cyber Security and Personal Data Protection" as opposed to the previous draft, the "African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa." Though the final outcome of the convention has yet to be released, we can only hope that the change of name is an indication of a shift in focus to personal data protection and that the human rights concerns highlighted above are addressed. However, given the opacity of the process, it is hard to know.

Source: *Access Now Blog*, June 02, 2014

Cyber Governance

Google search results may indicate 'right to be forgotten' censorship

Google is planning to flag up search results it has censored following a controversial ruling that allows European citizens the right to demand information on them be erased.

The search engine is considering placing an alert at the bottom of each page where it has removed links in the wake of the landmark "right to be forgotten" ruling last month.

The decision by Europe's highest court allows people living in Europe to ask for links to "inadequate, irrelevant or no longer relevant" material to be removed from search results, although it will still be available on the original web page.

Google has since been deluged with tens of thousands of requests from internet users to take down sensitive information on them since the ruling by the European court of justice (ECJ) on 13 May.

It is understood Google is planning to flag censored search results in a similar way to how it alerts users to takedown requests over copyright infringing material. For example, a Google search for "Adele MP3" shows that it has removed a number of results from that page after receiving complaints under the US Digital Millennium Copyright Act.

Google is also planning to include information about "right to be forgotten" removals in its biannual transparency report, which reveals the number of government requests worldwide to remove material from its search results.

Google said last Monday that it had so far received 41,000 requests to take down sensitive material from people in Europe since the landmark ruling, including a politician with a murky past, a convicted paedophile and a man who had attempted to murder his family and wanted to remove links about his crime. Google chief executive Larry Page has said that nearly a third of the 41,000 requests received related to a fraud or scram, one fifth concerned serious crime, and 12% are connected to child pornography arrests.

The search company, which launched an online form two weeks ago for people wanting to airbrush material about their past, does not have to comply with every request, but must consider whether removing information is in the public interest.

Google has set up an advisory committee to issue recommendations about where the boundaries of the public interest lie in the requests, made up of seven people including its executive chairman Eric Schmidt and Wikipedia founder Jimmy Wales.

Wales has described the ECJ ruling as censorship and raised concerns that news organisations would be particularly affected because Google is the primary source through which internet users find information. In an interview with the technology site TechCrunch on this weekend, Wales said: "I think the decision will have no impact on people's right to privacy, because I don't regard truthful information in court records published by court order in a newspaper to be private information. If anything, the decision is likely to simply muddle the interesting philosophical questions and make it more difficult to make real progress on privacy issues.

"In the case of truthful, non-defamatory information obtained legally, I think there is no possibility of any defensible 'right' to censor what other people are saying."

Google declined to comment.

Jodie Ginsberg, chief executive of Index on Censorship, said: "The fact that Google plans to add 'flags' to search links it has removed does nothing to tackle the fundamental problem with the 'right to be forgotten' ruling - which is the complete absence of legal oversight in this process.

"We remain deeply concerned about a ruling that opens the door to a censoring of the past without any proper checks and balances."

Source: *The Guardian*, June 8, 2014

Google and Facebook can be legally intercepted, says UK spy boss

UK intelligence service GCHQ can legally snoop on British use of Google, Facebook and web-based email without specific warrants because the firms are based abroad, the government has said.

Classed as "external communications", such activity can be covered by a broad warrant and intercepted without extra clearance, spy boss Charles Farr said.

The policy was revealed as part of a legal battle with campaign group Privacy International (PI).

PI labelled the policy "patronising".

It is the first time the UK has commented on how its legal framework allows the mass interception of communications, as outlined by US whistleblower Edward Snowden in his leaks about global government surveillance.

The former National Security Agency contractor revealed extensive details of internet and phone snooping and has since fled the US and sought temporary asylum in Russia.

Charles Farr, director general of the Office for Security and Counter-Terrorism, told PI that Facebook, Twitter, YouTube and web searches on Google - as well as webmail services such as Hotmail and Yahoo - were classified as "external communications", which meant they could be intercepted without the need for additional legal clearance.

Internal communications between citizens can only be intercepted when a targeted warrant is issued. Warrants must be signed by a minister and can only be issued when there is suspicion of illegal activity.

But when someone searches for something on Google or posts on Facebook they are sending information overseas - constituting an act of external communication that could be collected under a broader warrant which does not need to be signed by a minister, explained Mr Farr in a 48-page written statement.

However, he said data collected in this way "cannot be read, looked at or listened to" except in strictly limited circumstances.

Mr Farr said there was a "significant distinction" between intercepting material and a person actually reading, looking at or listening it.

Although this is the first time Mr Farr has publicly commented on the matter, the issue was previously raised by privacy researcher Caspar Bowden.

He briefed the House of Lords in 2000 ahead of the Regulation of Investigatory Powers Act coming into effect, which granted GCHQ the relevant power.

However, he told the BBC that his testimony was only presented to a near-empty House of Lords and was not reported outside of Hansard.

Analysis - Gordon Corera, security correspondent

British intelligence has always said that its activities are lawful.

But one of the problems has been that the law surrounding interception is incredibly hard to understand. Charles Farr's statement provides new details of how the government believes it applies to different forms of communications.

It reveals that a Google search by someone in Britain may be considered an external communication because the request and the result go abroad to Google's computers.

That means it could be swept up under the broader warrant covering "external "communications.

However, Mr Farr says that actually reading or examining a Briton's communications swept up in this way would still require a domestic, more targeted warrant.

Much of the debate over whether the state does conduct mass surveillance comes down to a central question - does the act of computers collecting information constitute surveillance or does it take a person reading or accessing that data for someone's privacy to be invaded?

Speak to privacy advocates and government officials and you get a radically different answer.

Mr Farr did not reveal the extent to which GCHQ used its power to intercept external communications.

In a statement, GCHQ said all its work was "carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate".

'Byzantine' laws

But civil liberty groups were outraged by the revelations.

James Welch, legal director of human rights group Liberty, said: "The security services consider that they're entitled to read, listen and analyse all our communications on Facebook, Google and other US-based platforms.

"If there was any remaining doubt that our snooping laws need a radical overhaul there can be no longer."

Meanwhile, Eric King, deputy director of Privacy International, said the revelation showed that spy agencies operated under their own laws.

"Intelligence agencies cannot be considered accountable to Parliament and to the public they serve when their actions are obfuscated through secret interpretations of Byzantine laws."

But some others did not find the revelations surprising.

Alan Woodward, a security expert who has undertaken consultancy work for GCHQ, said: "I think what is happening is that people are just becoming familiar with legislation that has been in place for many years, probably because of all the civil liberty groups raising concerns. As you can see from the Act, it has never been a secret.

"The bit that people tend to forget is that RIPA [Regulation of Investigatory Powers] has protections as well, something you won't find in many other countries. The difference in the UK is that civil liberty organisations have the right to challenge these things, a right which they would not have in, say, Russia."

However, Mr Bowden suggested the relevant statute had been obscurely worded.

"Interpreting that section requires the unravelling of a triple-nested inversion of meanings across six cross-referenced subsections, linked to a dozen other cross-linked definitions, which are all dependent on a highly ambiguous 'notwithstanding'," he said.

The legal challenge, brought by PI, Amnesty, the American Civil Liberties Union and six other national civil liberties organisations, was a direct response to the revelations made by Mr Snowden about the UK's global digital surveillance.

Source: *BBC News*, June 17, 2014

France lashes out at internet naming body ICANN

France has launched a strong attack on the US-based international body that governs internet addresses, calling its decision-making “totally opaque” and saying a move to assign domain names for wine could threaten talks on a transatlantic trade deal.

Paris will demand a big shake-up of Icann – the Internet Corporation for Assigned Names and Numbers – at a meeting of its government advisory committee in London on Monday, calling for a bigger say for states in its governance.

France's anger has been triggered by a decision this year by Icann to go ahead with the launch of the two domain names .vin and .wine, which critics say could undermine international agreements on so-called geographical indicators that restrict the use of labels, such as champagne and other area-specific wines and foods.

The European Commission,France, the UK and Spain have all appealed to Icann to halt the procedure on the two domain names unless safeguards for geographical indicators are assured.

But France has linked the issue to the broader question of how Icann is structured and governed.

"The problem is it is totally opaque, there is no transparency at all in the process," Axelle Lemaire, minister for digital affairs, told the Financial Times.

In a letter to Manuel Barroso, European Commission head, this month, Ms Lemaire and two senior ministers argued that the domain names could prejudice EU-US trade talks in which France and other countries are anxious to preserve geographical indicator rights. These stop, for example, American producers calling sparkling wine champagne, or blue cheese Roquefort.

"These decisions could imperil the current talks on the transatlantic [trade] partnership by forcing the imposition of a model by the means of technical discussions on internet naming," they wrote.

Their worry is that a private company which acquired the domain names could market products via, for example, a "champagne.wine" website that were not authentic champagne, without legal recourse.

Ms Lemaire also wrote this month to the Icann board saying the domain name process threatened to "undermine confidence in your organisation".

The US agreed this year to give up its ultimate control of Icann exercised through the commerce department, but Ms Lemaire made clear France wants to go further, seeking to rally support for a global conference on its overhaul.

Paris wants it set up under international law with a redefined mission and overseen by a "general assembly" of stakeholders that would include governmental representation on a "one country, one vote" basis, Ms Lemaire said.

In her letter to the Icann board she wrote: "The lack of adequate redress mechanisms and, above all, the lack of accountability demonstrate the need for significant reform of Icann even before the current debate on the global internet governance system comes to a conclusion."

Icann, founded in 1998, is a non-profit making organisation grouping private sector, public sector and technical interests in what it calls a "bottom-up, consensus-driven, multi-stakeholder model".

Three years ago, Icann decided to lift most restrictions on the naming of top level domains. It has since received applications for almost 2,000 new domains and has already delegated about 300 of them, including .beer,london and .luxury. Among the new domains are ones using non-Latin characters such as Arabic and Chinese.

The process has not been without controversy. Some corporations are worried that they will need to spend large amounts of money buying addresses in the new domains in order to protect their trademarks from cybersquatters or fraudsters.

Others are worried about the potential consequences of generic terms such as .search or .music falling under the control of a single corporation. Google and Amazon are among 13 organisations competing for the domain .app.

Source: *The Financial Times*, June 22, 2014

India's only cyber appellate tribunal defunct since 2011

The first and only cyber appellate tribunal in the country has been lying defunct for the last three years. The tribunal has not adjudicated a single case since June 30, 2011 when the previous chairperson Justice Rajesh Tandon retired.

Each case that comes to the tribunal has been adjourned on the ground that there is non-availability of the chairperson and the member (judicial) to pass judicial orders.

When the tribunal was setup in October 2006, it was seen as a specialised forum to redress cyber frauds.

It was conceived to adjudicate cyber crimes and disputes such as hacking, sending of offensive or false messages, receiving stolen computer resource, identity theft, cheating by personation, violation of privacy, domain name disputes and other cyber fraud cases.

However, the tribunal has been vested with the same powers as a civil court, the cases requiring punishment instead of financial penalty are transferred to the magistrate concerned. But, this does not explain the dismal number of cases filed at the tribunal. As of today, there are only 32 cases pending at the tribunal. Four cases were admitted in 2012, ten last year, and eight in 2014.

A survey conducted recently by the Internet and Mobile Association of India (IAMAI), projected that the Internet user base in the country is to touch 243 million by June 2014. This growth of Internet users has also led to a substantial growth in other digital industries such as e-commerce. This has led to a spurt in cyber frauds cases.

As per latest data available with the National Crime Record Bureau (NCRB), a total of 2876 cases were registered under the Information Technology Act in 2012, a sharp increase from 1791 in 2011.

But not all cyber fraud cases are reported.

This seems to be true for not only individuals but also for companies.

There is very little knowledge on the different kinds of cyber crimes, the laws governing them, and the redressal forums.

And the national appellate tribunal remaining non-functional for three years has not helped either, as it has forced cyber fraud victims to approach the high courts, which are already overburdened with case pendency, for remedy.

Central government counsel Sumeet Pushkarna said the selection of the chairperson and members of the tribunal is made by the Centre in consultation with the Chief Justice of India. He had informed the Delhi HC on May 29 that it will take eight weeks to appoint the chairperson.

Source: The Hindustan Times, June 29, 2014

Kenya Internet Governance Forum (IGF) set for July 3 in Nairobi

The 2014 edition of the Kenya Internet Governance Forum (IGF) will be held on Thursday July 3, 2014 at Strathmore University.

Like previous sessions, the day-long meeting will be preceded by an online discussion whose report will be ratified during the face-to-face meeting.

This year's Kenya IGF - with the theme Connecting Counties for Enhanced Multi-stakeholder Internet Governance - is to be convened by the Kenya-chapter of Internet Society (ISOC-Kenya) in partnership with the Kenya Internet Governance working group.

The 2014 Kenya IGF will focus on various key thematic areas including: Policies enabling access/Net Neutrality; Cyber security; Internet as an engine for growth and development focusing on Internet and Human rights as well as social media and hate speech.

The 2014 Kenya IGF comes after the recent launch of the National Cybersecurity Framework which takes into account the legislative and regulatory provisions on cyber security in the country as well as other provisions in the international cybercrime conventions. The Cybersecurity Framework recognizes the role of key players including law enforcement agencies, various government agencies, the private sector and academia, among others stakeholders.

The strategy - which defines Kenya's cybersecurity vision and emphasizes on the commitment to support national priorities - recognises the combined critical

role of various government agencies including Communications Authority of Kenya (CAK), ICT Authority, the National Intelligence Service as well as the private sector.

The framework incorporates a Public Key Infrastructure (PKI) that will facilitate the creation, storage and distribution of digital certificates. The PKI is intended to safeguard the integrity of e-transactions and encourage adoption of this robust business platform.

The pre-event online discussion is being held over a period of three days - from July 26 - 28. The draft programme for the Kenya Internet governance forum is available on the Kenya Internet Governance Forum website.

Source: *AllAfrica,* June 27, 2014

Germany nixing verizon contract highlights economic impact Of US spying

The German government announced it was pulling its contract with Verizon due to fears the Internet provider was allowing U.S. agencies to spy on the government's communications, the Associated Press reported Thursday. The news highlights the negative impact controversial government surveillance programs have on American businesses abroad.

Reports of the U.S. spying on German citizens sparked backlash in Europe last year in the wake of leaks from former government contractor Edward Snowden about the scope of NSA surveillance programs. News that German Chancellor Angela Merkel was targeted by the programs strained relations between the two nations.

"There are indications that Verizon is legally required to provide certain things to the NSA, and that's one of the reasons the cooperation with Verizon won't continue," Interior Ministry spokesman Tobias Plate told the Associated Press.

The announcement demonstrates the controversial surveillance practices are bad for American businesses. In the aftermath of the Snowden leaks, tech companies from Verizon to Facebook have had to defend their companies practices to angry customers in the U.S. and abroad concerned they are sharing personal data with the U.S. government. Companies from Microsoft to Apple have called on the government to make reforms.

Verizon Germany's managing director Detlef Eppig released a statement to TechCrunch, "Verizon Germany is a German company and we comply with German law."

The company outlines its "position on the inability of the U.S. government to access customer data stored outside the U.S." on its policy blog. According to the post, Verizon did not receive any demands from the U.S. government for data stored in other countries. It goes on to say the U.S. can't compel Verizon to produce data stored in centers outside the U.S., and if it tried to, the company could challenge that in court.

The current contract between Germany and Verizon will expire in 2015, the AP reported.

Germany has a history of leading European countries in the promotion of data privacy rights and online freedoms. Their strict policies have presented challenges for American companies like Facebook and Google.

The news comes on the heels of U.S. attempts to repair the blows the Snowden documents caused to its relationships with EU nations last year. On Wednesday the Obama administration pledged to pass legislation that would extend some of the personal privacy rights Americans have in U.S. courts to EU citizens.

When Merkel visited the U.S. in May, she told Obama it was too soon to return to "business as usual" in the wake of the NSA revelations. The announcement shows that's not changing soon.

Source: *TechCrunch,* June 26, 2014

'Double 7' strategy may give China more control over internet: Duowei

China is deploying what is referred to as its "double seven" strategy in an attempt to take more control in the global governance of the internet, reports Duowei News, an outlet run by overseas Chinese.

Representatives of China are currently among the 3,300 people from 130 countries in London to attend the 50th global conference of the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization that coordinates the internet's global domain name system.

The corporation established in California in 1998, helps keep internet protocols in order by ensuring that each web address is not assigned more than once. The organization also facilitates the addition of top-level domains, which are suffixes to web addresses like ".com", ".org", and ".gov".

Lu Wei, chairperson of China's State Internet Information Office, said at the opening ceremony that global participants have now reached a general consensus over seven key issues of internet governance raised by China.

"We all hold one single aspiration, that is, to improve the governance of the internet. This is in line with ICANN's vision of 'One World, One Internet'," he said, adding that it is natural for countries to have different views due to different national situations, historical backgrounds, and internet governance systems. During his speech, Lu also expressed appreciation and support for the advancements of the multistakeholder model that framed April's NETmundial meeting in Sao Paulo, Brazil.

According to Chinese state media, this was the first time an official from a non-host country made a keynote speech at the ICANN conference.

Beijing observers say Chinese president Xi Jinping's decision to establish the central internet security and informatization leading group early this year signals a major effort by China to become more involved in a new world order of internet governance based on international cooperation and away from US control.According to Duowei, China has shown two notable characteristics in its efforts to increase its influence in global internet governance.

The first is deploying a two-pronged strategy known as the "double seven," in reference to China's so-called "seven baselines" and the aforementioned "seven consensuses." The seven baselines are observing domestic laws and regulations, the socialist system, national interests, the legitimate interests of citizens, social order, morality and information authenticity.

The seven consensuses are that the internet should be for the benefit of all mankind, that the internet should bring peace and security to all countries and not be used as a "weapon" to attack others, that the internet should serve the interests of developing countries, that the internet should focus on protecting the legitimate rights and interests of citizens and not become a hotbed for criminal activity or terrorism, that the internet should run with civility and integrity, and not drive rumors or perpetrate fraud, that the internet should pass on positive energy and carry forward the culture of mankind and finally, that the internet should aid in the healthy development of minors.

The second prong of China's strategy is to continue pushing for the US to relinquish the final vestiges of its authority over ICANN's functions, which it has maintained since the organization was formed nearly 16 years ago. A reduced role for the US, which has been welcomed by international critics and anticipated for more than a decade, would put an end to the long-running contract between the US commerce department and ICANN. That contract is set to expire next year but could be extended if the transition plan is not complete.

"We look forward to ICANN convening stakeholders across the global internet community to craft an appropriate transition plan," Lawrence E. Strickling, assistant secretary of commerce for communications and information, said in a statement in March.

Source: *Want China Times,* June 26, 2014

COMMENTARIES

Kenneth Chang, "Automating Cybersecurity", *The New York Times*, June 02, 2014

Amit R. Saksena, "India Scrambles on Cyber Security", *The Diplomat*, June 18, 2014

Jennifer Granick, "New Ruling Shows the NSA Can't Legally Justify Its Phone Spying Anymore", *Wired*, June 13, 2014

Des Houghton, "Why Cyber Bullying Must be Outlawed", *The Courier Mail*, June 14, 2014

Sen. Dan Coats, "Addressing Cyber Threats", *Kokomo Tribune*, June 18, 2014

Mark Sweney, "If Google can get rid of personal data, why can't it purge the pirates?", *The Guardian*, June 1, 2014

Connor Friedersdorf, "Is America Incapable of Regulating Robots", *The Atlantic*, June 28, 2014

Shannon Tiezzi, "China's Sovereign Internet", *The Diplomat*, June 24, 2014

Jayshree Bajoria, "India's Snooping and Snowden", *The Wall Street Journal*, June 05, 2014

JOURNAL ARTICLES

Scott Shackelford, and Amanda Craig,"Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity", *Stanford Journal of International Law*, Vol. 50, p. 119, Winter 2014

Kristen Eichensehr, "The Cyber-Law of Nations", *Georgetown Law Journal*, Vol. 103, No. 2, 2014

Roderic Broadhurst, Peter Grabosky, Mamoun Alazab and Steve Chon, "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime", *International Journal of Cyber Criminology*, Vol. 8, No.1, 2014

REPORT

Kevin Mickelberg , Laurie Schive and Neal Pollard, "US Cybercrime: Rising Risks, Reduced Readiness - Key Findings from the 2014 US State of Cybercrime Survey", *PricewaterhouseCoopers*, June 2014

"ASD Cyber Security Bulletin", *Australian Government, Department of Defense*, Issue 13, June 2014

"Latin America + Caribbean Cyber Security Trends", *Organization of American States & Symantec*, June 2014

"Net Losses: Estimating the Global Cost of Cybercrime", *McAfee &Centre for Strategic and International Studies (CSIS)*, June 2014

"Cyber Essential Schemes - Requirements for basic technical protection from cyber attacks", *Government of UK*, June 2014

Melody Patry, "Brazil: A new global internet referee?", *Index on Censorship,* June 2014

Aaron Shull, "Global Cybercrime: The Interplay of Politics and Law", Centre for International Governance Innovation, June 2014

Neelie KROES, Vice-President of the European Commission responsible for the digital agenda, on inclusive governance for a global internet

Brussels~ Tuesday, June 10, 2014

Across the world I have seen the role that new technology can play. This is not just a toy for the happy few. Across the world it can cut poverty, promote and protect fundamental rights, empower individuals and groups by connecting them to unlimited opportunity. And it so is a tool for equal opportunities between men and women.

I am committed to including as many people as possible in that digital opportunity. Every European digital. For boys and girls.

I know World Summit on Information Society is also dedicated to that goal.

And more than that: World Summit on Information Society is a living example of how governments, civil society and private companies can work together to bridge the digital divide.

The Internet is a platform for amazing innovation. Able to cope with diversity, and adapt to local needs and sensitivities.

Its main innovative success lies in its nature: open, unified and global. It deserves the governance to match. Open and transparent, global and multi-stakeholder. But we cannot go for he lowest common denominator, nor should we run off in separate directions. That would damage the network, and lessen its economic and social impact. Instead we should find a way forward together. We are in the middle of a significant transition in how the Internet is governed.

As you know – the United States government has announced they will transition core Internet functions for more open management and stronger accountability. I sincerely welcomed that announcement. But now the follow-up to that announcement is at stake.

Let's capture the opportunity. Let's find a clear position and a clear voice within this global debate.

In Europe we have already defended for a long time the multi-stakeholder model. But organisations must be accountable, transparent, and independent. Decision making must be more effective and more global. Structures must defend and promote our most basic rights and values.

For me there are three key objectives:

First, to make governance more inclusive. Especially of developing countries.

Second, to strengthen the multi-stakeholder approach to governance.

Third, to recognise the responsibilities that governments have in enforcing the rule of law, acting within that multi-stakeholder model.

I do not support government control of the Internet. Not by one government, not by a group of governments.

Public authorities do have responsibilities and duties. But self-regulation or similar is often more appropriate. And the stakeholders who design, run and use the Internet are at the heart of any governance system.

The NETmundial conference in Brazil gave us a great example of what the global multi-stakeholder community can achieve. The roadmap for internet governance was a welcome outcome for all those who care about an inclusive, digital future.

This work has been stuck for a number of years. I don't want that to continue.

So today I am calling on all of you for your help. Let's work together. There were very clear milestones in that roadmap: let's take them seriously.

But there are also principles to be upheld and to be defended. For example, we cannot speak about a vision for media in the Digital Age without clearly defending the principle of freedom of expression and the free flow of information.

Our approach must be – as was stated clearly in Sao Paulo – that rights that people have offline must also be protected online.

Let's remember the prize. A vibrant, unified digital world, diverse and democratic, developing and benefiting every corner of the globe, for girls and for boys, for men and for women

I hope that we can all agree on that. Let's not stay with the promise, let's put it into practise.

Source: *Europa Press Release*, June 10, 2014

Karen Bradley, Member of British Parliament, speech on UK cyber security to IA14 conference

London ~ Monday, June 16, 2014

Last year Verizon reported that most successful cyber attacks take a matter of hours to breach a system. Many take minutes or even just seconds.

The frightening fact for me, was that in some cases it is over a year until the compromise is discovered and in a large proportion of specific cases the victim discovers the compromise only through a third party for instance, the police, a security firm or even a competitor tells them.

We rely on the internet. We all conduct an increasing amount of our professional and personal lives online. A survey last year found that the average family owns six devices that provide access to the internet. Smart phones, tablets, laptops and TVs.

We're sending out personal data into cyberspace all day every day, through emails, passwords and via our bank accounts to name a few.

Combined with the fact that 72% of all adults in Great Britain bought goods or services online in 2013 , up from 53% in 2008, that presents the breadth of opportunity for cyber criminals.

This is why cyber crime, is a top threat to UK national security. It is up there with international terrorism.

This evening, I am delighted to be here today to talk to you about how the Serious and Organised Crime Strategy is prioritising work with our key partners to ensure that the UK is a safe place to do business online, and what more we can do together. For those who don't know me, I am Karen Bradley, the Minister responsible for Serious and Organised Crime and I head the team that is responsible for our work on cyber security in the Home Office.

Threat

As you heard from the Ciaran Martin earlier, Cyber crime is a global threat, operating across international borders.

Cyber crime is beginning to transform criminality in almost every country. And worse, it enables organised criminals to operate on a scale and at a pace which has previously been unthinkable.

Elaborate online markets are used to exchange information and skills that were once niche are now being exploited in the real world.

For example, last year a drugs trafficking network hired cyber criminals to alter cargo manifests at Antwerp, in an attempt to smuggle their goods in containers to the UK. It was particularly brazen since when the initial breach was discovered and a firewall installed to prevent further attacks, hackers broke into the premises and fitted key-logging devices onto computers.

Ultimately cyber crime is crime like any other. It occurs in the virtual world rather than the physical world but still impacts us directly. So how do we stay one step ahead of the cyber criminals and protect ourselves from attack, and pursue those who commit the crime?

I want to set out for you the priorities in the new Serious and Organised Crime Strategy and how it underpins activity to protect ourselves from attack, and pursue those who commit cyber crime.

Serious and Organised Crime Strategy

In October last year we launched the National Crime Agency and published the new Serious and Organised Crime Strategy. We have refined our approach to tackling serious and organised crime into four areas of focus: Pursue, Prevent, Protect and Prepare. This follows and reinforces the previous framework of our Counter-Terrorism Strategy, CONTEST.

PURSUE – prosecuting and disrupting organised crime groups. In other words, catching the bad guys.

PREVENT - stopping people from becoming involved in, and remaining involved in, serious and organised crime. In other words, stopping the bad guys from being bad guys.

PROTECT - reducing our vulnerability to harm from these groups by strengthening our systems and processes and providing advice to the private sector and the public. In other words, helping you and others to not become a victim of the bad guys.

And PREPARE – reducing the impact of serious and organised crime when it happens. So, helping victims and wider communities to recover when the criminals strike. I will focus today on the PURSUE and PROTECT areas of our work.

Pursue

We are changing the way we pursue cyber criminals. Law enforcement needs to have the right skills to respond to the ever evolving ways in which crime is being committed. But crime is still crime.

The National Crime Agency (NCA) leads the crime fighting response to the most serious incidents of cyber-dependant and cyber-enabled crime through its National Cyber Crime Unit (NCCU) and Commands including the Economic Crime Command. The NCA now works with regional and local policing. Through increased investment, new dedicated cyber and fraud units are being developed in our network of Regional Organised Crime Units, or ROCUs. And the College of Policing, now has a dedicated training programme to drive up cyber skills in local police forces. We will see a significant increase in the numbers of police officers and staff who have been trained by 2015.

There are real opportunities for industry and law enforcement to work together to build skills to tackle cyber crime, and to understand the changing threats. The ROCUs are establishing relationships with

businesses in their region, and the NCA's NCCU is sharing information on cyber attacks with the private sector. CERT UK is playing a vital role in sharing information through its CISP [Cyber-security Information Sharing Partnership] platform. But this is just a start. In addition to increasing law enforcement capabilities, we want to make the legislative response stronger. We published the Serious Crime Bill this month. This amends existing legislation, which will mean that those who are found guilty of committing cyber attacks which cause serious damage, including to the economy, face lengthy prison sentences. The Serious Crime Bill currently before Parliament, amends the Computer Misuse Act 1990, including to create a new offence of unauthorised acts in relation to a computer that result, either directly or indirectly, in serious damage to the economy, the environment, national security or human welfare, or creates a significant risk of such damage.

The offence will carry a maximum sentence of life imprisonment for cyber attacks which result in loss of life, serious illness or injury or serious damage to national security and 14 years' imprisonment for cyber attacks causing, or creating a significant risk of, severe economic or environmental damage or social disruption.

Although pursuing cyber criminals is important, we need to remember that behind statistics reporting billions of pounds lost from cyber attacks, are individual tragedies and victims. Whether it's a single individual or a large corporation. A large company may be able to absorb a loss of a few thousand pounds from a cyber attack. But for an SME, that could be the difference between folding or surviving. And these businesses will form part of your supply chains, and are an integral part of the industries we all depend on.

Pursue International

The UK cannot tackle cyber crime alone.

We need to work with our international partners in order to pursue the criminals and prevent this crime. That is why at the heart of NCA's approach to cutting cyber crime is international collaboration. Through its relationship with the European Cyber Crime Centre in Europol, and working closely with other international law enforcement agencies.

You will have seen the NCA's alert recently on the two week window to protect yourself and your business against two variants of malware, GameOverZeus and Cryptolocker.

This NCA alert is part of one of the largest industry and law enforcement collaborations attempted to date. This is a fantastic example of international collaboration to pursue cyber criminals across borders, and to protect the public and private sector from attacks.

I hope this gives you a better understanding of how we are strengthening our response to pursuing criminals who commit cyber crime. Working together with law enforcement is an important part of our work.

Protect

Although it is important to ensure we pursue criminals and their crimes, I am sure you would agree that it is better to protect ourselves and our systems from an attack than wait until our data, finances and confidence are stolen and compromised.

That is why Protect is a fundamental part of the Government response to the threat of cyber crime.

To quote from Sir Iain Lobban [Director GCHQ] "about 80% of known attacks would be defeated by embedding basic information security practices for your people, processes and technology."

Building on that message, this month, on 5th June we launched the Cyber Essentials Scheme, an industry-led organisational standard for cyber security, which gives a clear baseline to aim for in addressing cyber security risks to you and is designed to help combat cyber threats to SMEs in particular.

As Francis Maude has said, the Cyber Essentials scheme introduces good basic cyber security practices for businesses of any size, and in any sector. It applies to academia, charities, private and the public sector.

We want to see all organisations adopt the requirements. They are simple steps that can make a considerable and important reduction to cyber vulnerability.

Awareness Raising

Of course, no matter what you do, users of online products and services are exposed to risk and their cyber security vulnerabilities can increase the threat to your business. We are helping to reduce the vulnerabilities presented by individuals by raising awareness of how to stay safe online.

Cyber Streetwise, funded through the National Cyber Security Programme was launched earlier this year and is the government's national cyber security awareness campaign. It is helping individuals and small business to understand what they should do to enhance their security online. We will continue to promote this with a further phase of the campaign later this year to reach as many people and as many small businesses as possible. We want people to know the key things to do in order to act safely online, and to make it second nature to do these things.

Strength in numbers

Cyber criminals are increasingly organised, highly skilled and numerous. But as I look around the room tonight I see the expertise, the commitment and the access to thousands of highly skilled individuals we need to outwit the criminal gangs and shut them down.

What I want you to take away from this is to know that we, the government, see tackling cyber crime as a top priority. We are committed in our Serious and Organised Crime Strategy to ensure that the UK is one of the most secure places in the world to do business in cyberspace. But we need your help.

We need you to share your knowledge and experience and encourage others to do the same. And we need you to share it with us so we can understand the evolving threats problems and work with you on how to protect your businesses.

We need you to protect yourselves and your customers. We need you to promote the guidance that is out there. This event is a great opportunity to build on existing partnerships, and take stock of what more needs to be done. I hope your time at this event today and tomorrow is worthwhile and productive.

Thank you.

Source: *Home Office National Crime Agency UK*, May 19, 2014