**EVENT REPORT**

## 1 Executive summary

The annual Commonwealth Cybersecurity Forum 2016, organised by the Commonwealth Telecommunications Organisation (CTO) and hosted by British Telecom (BT), was held from 23 to 24 March 2016 at BT Tower, London, United Kingdom.

The objective of the conference was to build international cooperation bringing together cybersecurity stakeholders from across the Commonwealth. The key outcome of the Commonwealth Cybersecurity Forum 2016 was to establish a clear understanding about the need for an effective national cybersecurity strategy for each and every Commonwealth country.

The Forum was attended by around 110 participants representing 25 Countries. It was conducted in 11 sessions, 24 presentations and 11 panel discussions with 58 resource persons. The programme of the event is in the annex of this report.

## 2 Opening ceremony

**Les Andersen**, Vice-President of Cyber, BT Security, UK: Partnerships are at the heart of the fight against cyberterrorism and cybercrimes due to the borderless nature of cyber. He stretched upon having adequate policies in place for the security apparatuses as a proactive and pre-emptive measure.

**Nigel Hickson**, Vice-President, IGO Engagement, ICANN: Good progress has been made in the transition of the stewardship of the Internet Assigned Numbers Authority (IANA) to a Global Multi-stakeholder partnership. ICANN supports the Internet Governance ecosystem, and considers the stability, security and openness of the Internet to be of paramount importance.

**Shola Taylor**, Secretary-General, CTO: Under its new strategic plan, the CTO has identified six strategic goals of which cybersecurity is one, where the Commonwealth, led by the CTO, has a central role in facilitating cooperation. The Commonwealth Cybergovernance Model developed by the CTO draws on the Commonwealth Charter, which provides a sound underpinning for the Commonwealth countries to cooperate in cybersecurity.

## 3 Session-one: Establishing an effective national cybersecurity strategy

**Chair: Mike St. John-Green**, Independent Cybersecurity Consultant, UK

This session examined the importance of a National Cybersecurity Strategy for a safe and secure cyberspace.

**Key outcomes:**

- Cybersecurity strategies are critical as ICT usage is increasing constantly and cyberattacks, including on critical information infrastructure, are proliferating locally and regionally. Moreover countries need to be up to a reasonable standard to be a partner of global e-economy.
- The development of the strategy should be carried out in a coordinated under a multi-sector approach with a national champion leading the work and identified relevant agencies driving the process.
  - A multi-stakeholder approach will harmonise efforts of all stakeholders and optimise resources.
- There are lot of models, tools and resources by various organisations e.g. ITU, UNCTAD, CTO, OECD, OAS, ENISA, Microsoft, etc. These, in synergy, can be used as a starting point in developing cybersecurity strategy.
- and challenges in implementing national cybersecurity strategies could be minimized by:
  - Assuring high-level national leadership;
  - Using national values as the basis for cybersecurity strategies;
  - Aligning cybersecurity policy and legal framework to national developmental goals;
  - Implementing a National governance framework (involving National CIRT);
  - Conducting national awareness/capacity building programmes and standards;
  - Securing adequate funding and resourcing; and
  - Engaging with regional and international partners.

- Cybersecurity strategy should focus on protecting the critical infrastructures. The definition of critical infrastructure needs to be broadened to include organisations that hold sensitive data, organisations that are iconic but not necessarily critical and organisations which hold the key to economic security.
- Initial step in developing a cybersecurity strategy should be to conduct a situational assessment which may focus on policy, strategy and organisation; legal and regulatory frameworks; incident response and management; culture and capacity; and funding and resourcing.
- Government needs to take a more interventionist approach because of its unique position and strengths. Cybersecurity strategy should not focus solely on crime.
- The leading organisation, mandated to implement the cybersecurity strategy, should be founded on appropriate legislative framework that would define and clarify roles and responsibilities and should have the power to effectively deliver its mandate.
- The civil society should be engaged in the strategy development phase.
- Model strategies (ITU, CTO, ENISSA, etc.) provide only guidance such as on strategic goals, specific objectives, strategies and actions. However the strategy should be developed based on a risk assessment and the cybersecurity maturity of the country.

### 3.2 Session-two: Responding to cybercrime through cyberlaw harmonisation

**Chair: Dr Karen Brewer**, Secretary General, Commonwealth Magistrates and Judges Association, UK

This session addressed the needs of Cyberlaw harmonisation in order to respond to cybercrimes effectively and efficiently.

**Key outcomes:**

- Response to cyberattacks require the right balance between cybersecurity measures, robust law enforcement action and early stage intervention to actually deter young people's exposure to cybercrime.
- Law enforcement has a role in promoting awareness among the public and small business level. International coalition is critically important to combating cyber crimes.
- Among others, legal frameworks should address:
  - Protection of children online;
  - Retention of computer data;
  - Reporting of cyber attacks and data breaches;
  - Acquisition of electronic evidence and issues of admissibility; and
  - Data protection legislation.
- Legislation and regulation relating to cybercrime need to be harmonised across borders to prevent criminals from taking advantage of gaps across borders. UNODC has recently established a repository of cybercrime laws and lessons learned for the purpose of facilitating continued assessment of needs and criminal justice capabilities, and the delivery and coordination of technical assistance.

- Virtual currencies may contribute to the growth of cybercrime.
- Effective legal frameworks should be underpinned by policy frameworks that are relevant, responsive and reflective of national circumstances.

### 3.3 Session-three: Defending and Protecting Critical Information Infrastructure (CII)

**Chair: Lady Olga Maitland**, Chairman, Copenhagen Compliance

This session discussed defending and protecting critical information infrastructures (CII), such as the telecom infrastructures and how the public and private sectors can work together to protect CII.

**Key outcomes:**

- Common cyberattacks experienced include DDoS attacks, phishing attacks, DNS amplification attacks, security behaviours, malware etc.
- Approaches taken by BT that is protecting them from cyberthreats include cyberdefence operation; information assurance; technical security; physical security; policy, standards and compliance.
- Critical success factors in delivering secure network include:
  - Collaboration between actors;
  - A strategy based on addressing future challenges, not just today's or yesterday's threat;
  - Clear governance, roles and responsibilities;
  - "Built-in" strategy not "Bolt-on";
  - Openness and transparency on successes and failures; many "eyes and hands" from around the world to improve and enhance thinking our actions;
  - Continuous improvement.

### 3.4 Session-four: Internet governance

**Chair: Laura Hutchison**, Policy Executive, Nominet, UK

This session discussed governing and managing the internet and accountability in multi-stakeholder governance model.

**Key outcomes:**

- Three layers of digital governance are infrastructure layer (bottom), logical layer (middle) and economic and societal layer (top).
- Internet governance should bring together all actors such as civil society, business, government, academics, parliamentarians and users.
- Internet Governance Forum is an effective multi-stakeholder platform to deliberate internet governance issues at a strategic level, but not on technical and operational matters.
- Internet governance should be diverse, flexible, participatory, inclusive, effective, transparent and respect human rights and fundamental freedoms.

### 3.5 Session-five: International cooperation - bridging boundaries

**Chair: Nigel Hickson**, Vice-President, Internet Governmental Organisations Engagement, ICANN

This session discussed cybersecurity cooperation approaches across the borders, and vulnerabilities and dependencies in infrastructure.

**Key outcomes:**

- The incident response community cannot be successful in isolation. Cooperation and coordination is essential.
- Building confidence and cooperative relations with neighbouring countries is essential that will contribute to the global efforts to make cyberspace more secure.
- Capacity building, training and education of community members is essential.
- Exchange of best practices and of information on threats and vulnerabilities is important.
- Much of the world's critical infrastructure e.g. communications, air-transport, maritime shipping, financial services, weather and environmental monitoring and defence systems depend on space infrastructure. Cyber vulnerabilities in space infrastructure are serious risks for the ground-based critical infrastructure at national, regional and international levels.
- Highly regulated institutional responses such as government led approaches are likely to be too slow in developing security capability. On the other hand non regulated approaches, led by industry are more likely to be agile and responsive.

### 3.6 Session-six: Data privacy and security risks

**Chair: Professor Ian Walden**, Professor of Information and Communications Law, Queen Mary University of London, UK

This session discussed concepts and practices of privacy and data governance, including cross-border cooperation.

**Key outcomes:**

- Law has not been able to keep pace with the evolution of technology in the last two decades;
- Concepts and practices of data privacy differ from country to country and region to region;
- Approach to data governance should augment organisation's existing information security management systems and IT governance processes by specifying additional roles, tasks and technical tools that can help better protect data privacy and security while satisfying compliances;
- Many cybersecurity vulnerabilities are the result of poor quality software engineering;
- Software errors cause cybersecurity problems – e.g. buffer overflows, numeric overflows, SQL injection, cross-site scripting, weak cryptography design, etc. Poorly designed software tools leave users exposed. Thus risks should be addressed at the design stages;
- Better cybersecurity will require international co-operation by introducing product liability laws that require software to be secure, and facilitating a mature software profession based on sound computer science, maths and engineering principles;

- Privacy is not an absolute right. Governments may need access to citizen's data in order to provide safety and security.

### 3.7 Session-seven: Combating cyberterrorism

**Chair: Professor Babak Akhgar**, Director of Centre of Excellence in Terrorism Resilience, Intelligence and Organised Crime Research

This session discussed the terrorists' use of internet.

**Key outcomes:**

- Access to Cyberspace is one of the assets of terrorists. For example they use various applications such as Facebook, Skype, Viber and WhatsApp;
- International terrorist organisation use the internet essentially for three purposes – (i) to communicate (ii) to recruit, groom and radicalise and (iii) for propaganda;
- Intelligence should not only be concerned about the immediate perpetrators but also about their associates who are passively involved in the terrorist incident;
- Focus areas of Government Communications Headquarters (GCHQ) of UK to ensure cybersecurity are – (i) Signals intelligence, (ii) Cyber defence, (iii) Cybersecurity, and (iv) Information Security;
- In many cases there are appropriate and adequate laws to address cyber crimes, but the challenge is enforcement.

### 3.8 Session-eight: International cyber capacity building

**Chair: David van Duren**, Head, Global Forum on Cyber Expertise, The Netherlands

This session discussed international co-ordination in capacity building.

**Key outcomes:**

- Since the cyberspace is commonly shared by all, it is important to improve safety and security of all the stakeholders and countries in order to remain safe and secure as a whole;
- International security involves protection of common interests, and measures of confidence building. On the other hand, domestic security involves protection of national security, and prosperity and public safety. Both the components require supportive legal and policy frameworks, and regional and global cybersecurity cooperation;
- A nation should make adequate investments in capacity building;
- An appropriate legal framework is important to have a strong capacity building framework, and to develop a resource base;
- International co-ordination is difficult, but crucial. High-level dialogues are important in order to ensure an effective international coordination;
- Focus should be on increasing the knowledge and skill sets on the information security workforce;
- As cyberthreats become more diverse, persistent and sophisticated, there is a need for multi-stakeholders partnership in cybersecurity capacity building.

### 3.9 Session-nine: Economic growth and innovation in cyberspace

**Chair: Sandra Sargent**, Senior Operations Officer, The World Bank

This session discussed the creation of a secure environment for business and consumers, how the virtual currencies are being exploited by cyber criminals, and the potential of the digital economy.

**Key outcomes:**

- Most of the companies do not have any formal strategy to protect themselves from cyberattacks, leaving both businesses and consumers at risk;
- Combating cyber crimes require voluntary collaboration between the public and the private sectors;
- Cyber threats arise not only come from technology vulnerabilities, but also due to people in the form of employees, subcontractors, suppliers who may pose threats;
- Due to the growing popularity of Bitcoin it has become an attractive and profitable target for cybercriminals. By analyzing the block chain (record of transactions) and applying de-anonymizing strategies, virtual currency operators can help identify Cyberthreats.

### 3.10 Session-ten: Internet safety and the protection of vulnerable people online

**Chair: Mr Abhilash Nair**, Lecturer in Internet Law, University of Strathclyde

This session discussed child sexual abuse online, protecting victims, tackling illegal and explicit materials online.

**Key outcomes:**

- A country should have a legal framework to prosecute child sexual offenders, protect the victims, and promote a supportive and safer online environment for children and young people;
- Protecting children online is a global challenge, which needs to be addressed on a global scale. International co-operation is essential for sharing information in order to eliminate or mitigate risks to children and young people online, such as grooming;
- The three key ingredients to prevent grooming are legal frameworks, enforcement and preventative programmes consisting of (a) educational and awareness initiatives aimed at children, parents, professionals and law enforcement who work with children and (b) incentives to deploy preventive measures by Internet Service Providers and online platforms;
- Children should be aware of common online threats and the means to remain safe and secure. Parents should be aware of the early signs of threats such as grooming and steps to be taken in such situations;
- In many circumstances, grooming online is faster and anonymous and results in children trusting an online 'friend' more quickly than someone they had just met 'face to face';
- Approach for identifying online child abuser should be both proactive and reactive.

### 3.11 Session-eleven: Building a cyber secure culture

**Chair: Dr Jessica Barker**, Cybersecurity Consultant and Director, J L Barker Ltd., UK

This session discussed how to build the next generation of cyber professionals.

**Key outcomes:**

- Becoming a hacker is relatively easy, because tools and forums are readily available, and cyber ethics are not well understood. However becoming a cybersecurity professional is harder, because of a lack of role models, negative perceptions, lack of understanding of opportunities.
- The shortage of skilled professionals is global concern.
- UK conducted a Cyber Security Challenge in 2010, which is a series of national competitions, learning programmes, and networking initiatives designed to identify, inspire and create cybersecurity professionals. Cyber Security Challenge, acts as a catalyst for identifying skills, inspiring informing individuals about available education and training opportunities.
- Academic learning can bridge the cyber skills gap, attract talent, deliver continuous improvement, and develop a security profession.
- Reasons for shortage of cyber professionals include lack of awareness of cybersecurity careers, lack of suitable educational opportunities and competition in the job market and the inability of traditional recruitment practices to attract suitable candidates.