Critical Information Infrastructure Protection
A perspective & Reality from the Commonwealth

Commonwealth Cybersecurity Forum
BT Centre, London
22-24 April 2015

Dr Martin Koyabe
Head of Research & Consultancy
Commonwealth Telecommunication Organisation (CTO)

www.cto.int
Background of this work

Following the drafting of the Commonwealth Approach for National Cybersecurity Strategies, six regional workshops were held by CTO to build the capacity of stakeholders.
Acknowledgement

Foreign & Commonwealth Office

Supporter

Host Partner

www.cto.int
Understanding CIIP

General definition

- Critical Resources
- Critical Infrastructure
- Critical Information Infrastructure

Interdependencies
Today Critical Information Infrastructure Protection (CIIP)

- Focuses on protection of IT systems and assets
  - Telecoms, computers/software, Internet, interconnections & networks services

- Ensures **Confidentiality**, **Integrity** and **Availability**
  - Required 27/4 (365 days)
  - Part of the daily modern economy and the existence of any country
Examples of Critical Infrastructure Sectors

- European Commission (EC) provides an indicative list of 11 critical sectors

- Energy
- ICT
- Water
- Food
- Financial
- Health
- Civil Administration
- Public & Legal Order and Safety
- Transport
- Chemical and Nuclear Industry
- Space & Research
What CI do you prioritize for your country?

- CIIP identification & prioritisation can be challenging

Interdependencies
Understand requirements & complexity

- Understand the critical functions, infrastructure elements, and key resources necessary for
  - Delivering essential services
  - Maintaining the orderly operations if the economy
  - Ensure public safety.
CIIP deployment is technical & complex

- Need to understand dependencies & interdependencies
  - Especially vulnerabilities & how to mitigate cascading cyber attacks

(90%) 30 days outages are disastrous
(99%) 3 days outages are disastrous
(99.9%) 8 hr outages are disastrous
CIIP Workshops Conducted by CTO (2014-15)

- Yaounde, Cameroon
  - Feb 2015
- Nairobi, Kenya
  - Aug-Sep 2014
- Colombo, Sri Lanka/Dhaka, Bangladesh
  - Aug-Sep 2014
- Port Vila, Vanuatu
  - Sep-Oct 2014
- Georgetown, Barbados
  - Nov 2014
- Gaborone, Botswana
  - Mar 2015
- Gaborone, Botswana
  - Nov 2014

© Commonwealth Telecommunications Organisation | www.cto.int
<table>
<thead>
<tr>
<th>Host Partner</th>
<th>Participating Countries</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ministry of Energy, Immigration, Telecommunications and Investment of Barbados</td>
<td>Barbados, Turks &amp; Caicos, Cayman Island, Bermuda, Grenada &amp; Montserrat</td>
<td>35</td>
</tr>
</tbody>
</table>

Georgetown, Barbados
Nov 2014
### Host Partner
Ministry of Posts and Telecommunications, ITU, TRB, ANTIC, Interpol, ECCAS

### Participating Countries
Cameroon, Burundi, Angola, Central Africa Republic (CAR), Chad, Republic of Congo, DR Congo, Equatorial Guinea, Gabon, Nigeria, Ghana, Zambia, Senegal

### Number of Participants
> 300
<table>
<thead>
<tr>
<th>Host Partner</th>
<th>Participating Countries</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ministry of Transport and Communications</td>
<td>Botswana, South Africa, Swaziland, Lesotho, Mozambique</td>
<td>&gt; 60</td>
</tr>
</tbody>
</table>

Gaborone, Botswana
Mar 2015
## Eastern Africa Region CIIP Workshop (Nov 2014)

<table>
<thead>
<tr>
<th>Host Partner</th>
<th>Participating Countries</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications Authority of Kenya</td>
<td>Kenya, Uganda, Tanzania, Rwanda, Burundi &amp; Zimbabwe</td>
<td>&gt; 50</td>
</tr>
</tbody>
</table>

Nairobi, Kenya  
Nov 2014
## Southern Asia Region CIIP Workshop (Sep 2014)

### Host Partner
Bangladesh Telecommunications Regulatory Board & NITC in Sri Lanka

### Participating Countries
Sri Lanka & Bangladesh

### Number of Participants
- Bangladesh (20)
- Sri Lanka (40)

---

![Meeting at Colombo, Sri Lanka & Dhaka, Bangladesh Aug-Sep 2014](image)

© Commonwealth Telecommunications Organisation | www.cto.int
Experienced Cyber Threats (1/3)

- **Mobile phone fraud**
  - IMEI/SIM Card fraud & cloning

- **Financial fraud**
  - Developing & emerging market countries are becoming targets & source of malicious Internet activities

- **Software piracy and lack of updated software**
  - Home user PCs remain vulnerable to cyber attacks
Experienced Cyber Threats (2/3)

• Use of ICT to commit acts of terrorism
  – Planning, co-ordination, implementation and promotion. For example Boko Harum, ISIS, Al-Shabaab & Al-Qaida etc
  – Creates social-economical problem. For example, the recent Garissa University attack in Kenya – 148 people were killed.

Teenage girls in the UK who flew to Syria via Turkey
Experienced Cyber Threats (3/3)

- **Cyber attacks targeting government portals**
  - Defacement of websites, motivated by individual reasons
    - Nigeria defence HQ attacked for fighting Boko Haram
    - Ghana (gov.gh) portal attacked (11 out of 58 sites attacked)
    - Senegalese ICT agency site attacked, linked to Charlie Hebdo

- **Social media/Citizen data**
  - Reputation and defamation is a new form of cyber attack
  - Anonymity on social networks
  - Privacy & civil liberties vs. Government snooping (national security)
Policy, Legal & Regulatory Considerations

• National legal framework
  – Lack of Cybersecurity legislation is still an issue
  – Countries require relevant technology to support enforcement

• Regional harmonization of policy & legal frameworks
  – Global good, needs national, regional & international actions

• Co-ordination and corporation is a MUST
  – Cybersecurity is a cross-boundary issue
  – Needed to combat ICT fraud, hacking, child pornography and copyright infringement
  – Consistency in procedures and processes
Technology Considerations

• Development of infrastructure
  – Develop reliable, resilient and available connectivity

• Need to establish & enhance national CERTs
  – Create sectorial CERTs
    o Finance, Energy, Transport, Military, Maritime, SMEs etc
  – Harmonize regional CERTs or CIRTs
  – Cyber drills and preparation

• Establish national clouds
  – Encourage use of country Top Level Domain (TLD) names
Capacity building, Research & Innovation Considerations

• Cybersecurity is complex & challenging
  – Develop technical skills through training & collaborations
  – Use expertise especially from the Diaspora

• Cultivate a culture of Cybersecurity awareness
  – Some CERTs are not proactive enough
  – Limited capacity building initiatives among key stakeholders

• Good practice in Cyber governance
  – Encourage use of country Top Level Domain (TLD) names
  – Effective data protection act/law missing
The Way Forward Already

- Use the current experience to develop or improve National Cybersecurity Strategies for member countries
  - based on the Commonwealth Approach Model

- Solicit more suggestions on how to improve the current strategy documents.
  - CTO has created mailing lists for each region working group

- Create a portal where members can inform each other and exchange information related to Cybersecurity
  - Keep track of CTO’s progress in this space
Q & A Session

Further Information Contact:

Dr Martin Koyabe
Email: m.koyabe@cto.int
Tel: +44 (0) 208 600 3815 (Off)
+44 (0) 791 871 2490 (Mob)

Visit:
http://www.cto.int/priority-areas/cybersecurity/