Global Cybersecurity Agenda (GCA)
A framework for international cooperation

Alexander NTOKO
Head, Corporate Strategy Division
Growing Cybersecurity Threats

- ICTs have become an integral part of information society.
- ICT networks are regarded as basic national infrastructure.
- ICTs are also exposing our societies to the threat of cyberwar/cyberattacks.
- Vulnerability of national infrastructures increases as the use of ICTs take root.
- Cyber attacks on ICTs are borderless and can be launched from virtually anywhere.
- As global reliance on ICTs grows, so does vulnerability to attacks on critical infrastructures through cyberspace.

i.e., Attacks against computer systems in Georgia & Azerbaijan (2008), Brazil (2008), S.Korea and the US (2009), and Google/Twitter(2009)

“No geographical borders, no boundaries and tremendous destructive power”
National Responses

- Developing National Computer Incident Response Teams (CIRTs)
- Enhancing public-private partnerships to enhance expertise, knowledge, skills, resources & experience
- Enhancing International Cooperation
- Also, many governments are preparing themselves for “Cyber-defense” as well as “Cyber-offense”:
  
  **Cyberwarfare**
  - Network-based attack and/or defense
  - Building cyber capabilities as a part of conventional warfare, including cyber military outfits
  - Cultivating cyber tactics as a national resource
  - Educating citizens and raising awareness of cybersecurity problems
Key Cybersecurity Challenges

- Lack of adequate and interoperable national or regional legal frameworks
- Lack of secure software and ICT-based applications
- Lack of appropriate national and global organizational structures to deal with cyber incidents
- Lack of information security professionals and skills within governments; lack of basic awareness among users
- Lack of international cooperation between industry experts, law enforcements, regulators, academia & international organizations to address a global challenge
Global Cybersecurity Cooperation

The lack of cybersecurity is a global problem that cannot be solved by any single entity alone!

The world is faced with the challenging task of developing harmonized and comprehensive strategies at the global level and implementing these with the various relevant national, regional, and international stakeholders in the countries.
Introduction to ITU

- Leading UN specialized agency for information and communication technologies (ICTs).
- Founded in 1865, ITU is the oldest specialized agency in the UN system.
- Global focal point for governments and the private sector with 191 Member States, 900+ Sector Members and Associates.
- ITU Headquartered in Geneva, Switzerland; 11 regional/area offices and staff from nearly 100 countries.
ITU and Cybersecurity

- In 2003, world leaders at the World Summit on the Information Society (WSIS) entrusted ITU as sole facilitator for WSIS Action Line C5 - “Building Confidence and Security in the use of ICTs”

- Since the 2006 ITU Plenipotentiary Conference, ITU Secretary-General has set cybersecurity as one of his top three priorities

- On 17 May 2007, in response to the decision of the ITU Membership and in fulfillment of ITU’s role as sole facilitator for WSIS Action Line C5, ITU Secretary-General launched the Global Cybersecurity Agenda (GCA) – a framework for international cooperation in cybersecurity

- ITU World Conferences and the 2010 ITU Plenipotentiary Conference further strengthened the role of ITU in cybersecurity and endorsed the GCA as the ITU-wide strategy on international cooperation
The High-Level Expert Group (HLEG) on Cybersecurity was established in 2007. It is comprised of over 100 renowned experts from a broad range of backgrounds, sectors and geographical regions.

These experts worked tirelessly to formulate proposals to the ITU Secretary-General on strategies to curb cyberthreats, combat cybercrime and promote cybersecurity.

Its outputs include the Report of the Chairman of the HLEG, a set of strategic proposals, and the HLEG Global Strategic Report, which summarizes the HLEG’s work in seeking to promote cybersecurity around the world.
Global Cybersecurity Agenda (GCA)

- GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.

- GCA builds upon five pillars:
  1. Legal Measures
  2. Technical and Procedural Measures
  3. Organizational Structures
  4. Capacity Building
  5. International Cooperation

- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.
  - **H.E. Blaise Compaoré**, President of Burkina Faso, and **H.E. Dr Óscar Arias Sánchez**, Former President of the Republic of Costa Rica and Nobel Peace Laureate, are both Patrons of the GCA.
Collaboration towards A Global Strategy

“The world’s foremost cybersecurity alliance!”

- Within GCA, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) are pioneering the deployment of solutions and services to address cyber threats on a global scale.

- ITU-IMPACT’s endeavor is the first truly global multi-stakeholder and public-private alliance against cyber threats, staging its state-of-the-art facilities in Cyberjaya, Malaysia.

- An operational home of ITU’s Global Cyber Security Agenda (GCA), it supports 191 Member States and others with the expertise, facilities and resources to effectively enhance the global community’s capability and capacity to prevent, defend against and respond to cyber threats.
GCA and ITU-T Activities

ITU-T Study Group 17

- Lead Study Group for Telecommunication Security
- Mandate for Question 4/17 (Q.4/17): Cybersecurity
- Provides ICT Security Standards Roadmap
- Draft summaries of Study Group 17 recommendations
- Focus Group on Identity Management (IdM)
- Approved over 100 Recommendations on security for communication
- Facilitates collaboration among national Computer Incident Response Teams (CIRTs)

WTSA Resolutions

- ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008)
- ITU WTSA Resolution 58: Encourage the creation of national computer incident response teams, particularly for developing countries (Johannesburg, 2008)
GCA and ITU-D Activities

Assisting developing countries in bridging the digital divide by advancing the use of ICT-based networks, services and applications, and promoting cybersecurity

- ITU National Cybersecurity/CIIP Self-Assessment Tool
- ITU Botnet Mitigation Toolkit
- ITU Cybercrime Legislation Resources
- ITU-D Study Group Q 22/1: Securing information and communication networks: best practices for developing a culture of cybersecurity
- ITU Toolkit for Promoting a Culture of Cybersecurity
- Regional workshops and capacity building activities related to cybercrime legislation and enforcement
- A Background paper on Cybersecurity: “The Role and Responsibilities of an Effective Regulator” (Global Symposium for Regulators (GSR), November 2009)

WTDC Resolutions


“13. [...] the challenge of building confidence and trust in the availability, reliability, security and use of telecommunications/ICTs [...] can be addressed by promoting international coordination and cooperation in cybersecurity, taking into account, inter alia, the ITU Global Cybersecurity Agenda (GCA), as well as the development of related public policies and elaboration of legal and regulatory measures, including building capacity, to ensure cybersecurity, including online protection of children and women.”
GCA and ITU-R Activities

• Establish fundamental security principles for IMT-2000 (3G) networks

• Issue ITU-R Recommendation on security issues in network management architecture for digital satellite system and performance enhancements of transmission control protocol over satellite networks

ITU-R Recommendations

• Recommendation ITU-R S.1250: Network management architecture for digital satellite systems forming part of SDH transport networks in the fixed-satellite service
• Recommendation ITU-R S.1711: Performance enhancements of transmission control protocol over satellite networks
ITU’s Child Online Protection

- Under the GCA umbrella, ITU initiated the Child Online Protection initiative (COP) in November 2008.
- COP has been established as an international collaborative network for promoting the online protection of children and young people worldwide by providing guidance on safe online behavior.

**Key Objectives of COP**

- Identify risks and vulnerabilities to children in cyberspace
- Create awareness
- Develop practical tools to help minimize risk
- Share knowledge and experience
Launching COP Global Initiative

- In 2010 the President of Costa Rica, H.E. Laura Chinchilla, became the new patron of COP.
- Together with Costa Rica, the ITU Secretary-General launched the COP Global Initiative with high-level deliverables.

Through this initiative, ITU is taking the next steps to develop a cybersecurity strategy for child online safety, delivering significant national benefits.
Collaboration towards A Global Strategy

“The world’s foremost cybersecurity alliance!”

- Within GCA, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) are pioneering the deployment of solutions and services to address cyber threats on a global scale.

- ITU-IMPACT’s endeavor is the first truly global multi-stakeholder and public-private alliance against cyber threats, staging its state-of-the-art facilities in Cyberjaya, Malaysia.

- An operational home of ITU’s Global Cyber Security Agenda (GCA), it supports 191 Member States and others with the expertise, facilities and resources to effectively enhance the global community’s capability and capacity to prevent, defend against and respond to cyber threats.
What is IMPACT?

- The International Multilateral Partnership Against Cyber Threats (IMPACT) is the first global public–private partnership against cyberthreats.

What is the ITU–IMPACT Mandate?

- Under the GCA framework, ITU–IMPACT alliance provides an open partnership platform for international cooperation between governments, industry leaders, academia and law enforcement agencies in order to facilitate the establishment of cybersecurity strategies and critical information infrastructure protection, to enhance coordination and cooperation in securing cyberspace.

Why ITU–IMPACT Collaboration?

- While it is important to have a national strategy in the government agenda, this is often not enough to secure cyberspace, which cannot be defined by geographic borders.
- Most developing countries do not have the proper expertise and know-how required for effectively planning and implementing these strategies and structures.
ITU–IMPACT Collaboration

[Diagram with categories: Industry Experts, Academia, International Bodies, Think Tank]

IMPACT’s Global Alliances

Expertise | Technology | Skills | Resources | Experience

[Logos of ITU and IMPACT]

CYBERSECURITY SERVICE

191 ITU Member States
ITU–IMPACT has also developed a global partnership with major industries, academia, and international bodies.

- This partnership allows each country to strengthen its capability to protect the security of national ICT infrastructure.
# ITU-IMPACT

## International Advisory Board

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. Hamadoun Touré</td>
<td>Secretary General of International Telecommunications Union (ITU)</td>
</tr>
<tr>
<td>Eugene Kaspersky</td>
<td>Founder and CEO of Kaspersky Lab</td>
</tr>
<tr>
<td>Mikko Hypponen</td>
<td>Chief Research Officer of F-Secure</td>
</tr>
<tr>
<td>Steve Chang</td>
<td>Founder and Chairman of Trend Micro</td>
</tr>
<tr>
<td>Ayman Hariri</td>
<td>Chairman of Oger Systems</td>
</tr>
<tr>
<td>John W. Thompson</td>
<td>Chairman of Symantec Corporation</td>
</tr>
<tr>
<td>Prof. Fred Piper</td>
<td>Cryptologist, Founder of the Information Security Group at Royal Holloway, University of London</td>
</tr>
</tbody>
</table>
ITU–IMPACT Activities

The ITU is facilitating the implementation process, managing communication and needs assessment with Member States and coordinating with IMPACT, to ensure effective delivery of the services provided.

Global Response Centre
Global Early Warning System, detecting and monitoring cyber-threats

National CIRT
Computer Incident Response Teams (CIRTs) and Incident Management capabilities at National level

Capacity Building
- Capacity building and training, on-site, on-line, and training on the job
- Regional workshops and events, to ensure sustainability and operations of the solutions
- Direct assistance to countries, to map the deployment with the needs of the Administration
Main Objectives: GRC acts as the foremost cyber threat resource centre for the global community. It provides emergency response to facilitate identification of cyber threats and sharing of resources to assist Member States.

Two Prime Highlights

NEWS (Network Early Warning System)
- Information collaboration platform providing
  - Real time threat monitoring and assessment
  - Statistical cyber threat trend analysis
  - Malware threat centre

ESCAPE (Electronically Secure Collaboration Application Platform for Experts)
- A collaborative platform for authorized cyber experts to pool resources and remotely collaborate with each other in a secure and trusted environment
- A comprehensive and growing database of key resources around the world
In just over one year, **nearly 70 countries**, out of a potential 191 countries, have confirmed their agreement to join ITU-IMPACT:

<table>
<thead>
<tr>
<th>No.</th>
<th>Partner Countries</th>
<th>No.</th>
<th>Partner Countries</th>
<th>No.</th>
<th>Partner Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Afghanistan</td>
<td>24</td>
<td>Indonesia</td>
<td>47</td>
<td>Senegal</td>
</tr>
<tr>
<td>2</td>
<td>Albania</td>
<td>25</td>
<td>Iraq</td>
<td>48</td>
<td>Serbia</td>
</tr>
<tr>
<td>3</td>
<td>Andorra</td>
<td>26</td>
<td>Israel</td>
<td>49</td>
<td>South Africa</td>
</tr>
<tr>
<td>4</td>
<td>Armenian</td>
<td>27</td>
<td>Italy</td>
<td>50</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>5</td>
<td>Austria</td>
<td>28</td>
<td>Jordan</td>
<td>51</td>
<td>Sudan</td>
</tr>
<tr>
<td>6</td>
<td>Azerbaijan</td>
<td>29</td>
<td>Kenya</td>
<td>52</td>
<td>Sweden</td>
</tr>
<tr>
<td>7</td>
<td>Bangladesh</td>
<td>30</td>
<td>Laos</td>
<td>53</td>
<td>Switzerland</td>
</tr>
<tr>
<td>8</td>
<td>Benin</td>
<td>31</td>
<td>Malaysia</td>
<td>54</td>
<td>Seychelles</td>
</tr>
<tr>
<td>9</td>
<td>Bhutan</td>
<td>32</td>
<td>Maldives</td>
<td>55</td>
<td>Syria</td>
</tr>
<tr>
<td>10</td>
<td>Bosnia &amp; Herzegovina</td>
<td>33</td>
<td>Mali</td>
<td>56</td>
<td>Tanzania</td>
</tr>
<tr>
<td>11</td>
<td>Brazil</td>
<td>34</td>
<td>Mauritius</td>
<td>57</td>
<td>Thailand</td>
</tr>
<tr>
<td>12</td>
<td>Bulgaria</td>
<td>35</td>
<td>Moldova</td>
<td>58</td>
<td>Tunisia</td>
</tr>
<tr>
<td>13</td>
<td>Burkina Faso</td>
<td>36</td>
<td>Montenegro</td>
<td>59</td>
<td>Turkey</td>
</tr>
<tr>
<td>14</td>
<td>Cameroon</td>
<td>37</td>
<td>Morocco</td>
<td>60</td>
<td>UAE</td>
</tr>
<tr>
<td>15</td>
<td>Cape Verde</td>
<td>38</td>
<td>Myanmar</td>
<td>61</td>
<td>Uganda</td>
</tr>
<tr>
<td>16</td>
<td>Chad</td>
<td>39</td>
<td>Nepal</td>
<td>62</td>
<td>Vatican City</td>
</tr>
<tr>
<td>17</td>
<td>Costa Rica</td>
<td>40</td>
<td>Nigeria</td>
<td>63</td>
<td>Venezuela</td>
</tr>
<tr>
<td>18</td>
<td>Côte d'Ivoire</td>
<td>41</td>
<td>Oman</td>
<td>64</td>
<td>Vietnam</td>
</tr>
<tr>
<td>19</td>
<td>Democratic Republic of Congo</td>
<td></td>
<td></td>
<td>65</td>
<td>Yemen</td>
</tr>
<tr>
<td>20</td>
<td>Egypt</td>
<td>42</td>
<td>Philippines</td>
<td>66</td>
<td>Zambia</td>
</tr>
<tr>
<td>21</td>
<td>Gabon</td>
<td>43</td>
<td>Poland</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Ghana</td>
<td>44</td>
<td>Romania</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>India</td>
<td>45</td>
<td>Rwanda</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>46</td>
<td>Saudi Arabia</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Establishing National CIRTs

**Main objectives:** To provide Incident Management, Advisories and Mailing List services, integrated with the Global Response Centre

- Incident Response and Handling
- Vulnerability Analysis and Handling
- Alerts and Warnings
- Technology Watch
- Training and Awareness

ITU supports countries in the implementation of the National CIRT through the establishment of the overarching policy framework to support this technical solution and related watch, warning and incident response capabilities as part of a national strategy.
ITU–IMPACT CIRT activities

- Objectives:
  - To assist partner countries’ assessment of its readiness to implement a National CIRT.
  - IMPACT reports on key issues and analysis, recommending a phased implementation plan for National CIRT.
  - Training courses for capacity building also provided.
  - In later stages the national CIRT will also be provided with enabling tools.

<table>
<thead>
<tr>
<th>No.</th>
<th>Partner Countries</th>
<th>Assessment Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Afghanistan</td>
<td>Completed in November 2009</td>
</tr>
<tr>
<td>2</td>
<td>Uganda, Tanzania, Kenya &amp; Zambia</td>
<td>Completed in April 2010</td>
</tr>
<tr>
<td>3</td>
<td>Nigeria, Burkina Faso, Ghana &amp; Ivory Coast</td>
<td>Completed in May 2010</td>
</tr>
<tr>
<td>4</td>
<td>Maldives, Bhutan, Nepal &amp; Bangladesh</td>
<td>Completed in June 2010</td>
</tr>
<tr>
<td>5</td>
<td>Serbia, Montenegro, Bosnia, Albania</td>
<td>Completed in November 2010</td>
</tr>
<tr>
<td>6</td>
<td>Cameroon, Chad, Gabon, Congo</td>
<td>Completed in December 2010</td>
</tr>
<tr>
<td>7</td>
<td>South America and Arab region</td>
<td>Planned in 2011</td>
</tr>
</tbody>
</table>

Following the assessment exercises, ITU is now moving to the implementation phase, according to requests for assistance from Member States.
ITU–IMPACT Cybersecurity Assessments

- ITU-IMPACT Cybersecurity workshop in Kabul, Afghanistan (October, 2009)
- ITU-IMPACT Cybersecurity workshop for East Africa: Kenya, Tanzania, Uganda and Zambia (26 – 29 April, 2010)
- ITU-IMPACT Cybersecurity workshop for Bhutan & Bangladesh (1 – 11 June, 2010)
ITU–IMPACT
Training and Skills Development

- IMPACT-Microsoft Network Forensics & Investigation Course: 6–9 April 2010 (Brunei)
  Closed session for law enforcement agencies – 4 countries participated

- IMPACT Network Forensics Course: 3rd – 7th May 2010 (IMPACT Global HQ)
  Class conducted for 22 participants from 5 countries

- IMPACT-SANS IPv6 Training: 26th May 2010 (IMPACT Global HQ)
  Training conducted by Dr Ullrich (SANS Internet Storm Center) – 72 participants
ITU–IMPACT
Partner Engagement

- IMPACT-Microsoft Critical Information Infrastructure Protection Seminar – December 2009
  - Session conducted by Angela McKay – Microsoft Corporation, US

- IMPACT-Trend Micro seminar on “The Botnet Storm: Challenges & Global Cooperation” – 14th April 2010
  - Session conducted by Raimund Genes, CTO of Trend Micro

- IMPACT-Kaspersky Seminar on Formulating Effective Global Counter-Phishing Efforts, 3rd March 2010
  - Session conducted by Michael Molsner, Malware Analyst, Kaspersky Lab, Japan
  - Session conducted by Dr Eric Cole, SANS Faculty Fellow & CTO of McAfee together with John Strand, SANS Certified Instructor

  - Session conducted by Dr. Jaan Priisalu, Co-Founder of CyberDefense League, Estonia & Mike Gault, CEO, GuardTime, Estonia

- IMPACT-Kaspersky Media Roundtable. IMPACT Chairman, Datuk Mohd Noor Amin & Kaspersky Founder, Eugene Kaspersky
  - Session held at St Regis Hotel, Singapore, October 2009

- IMPACT-Symantec Media Roundtable. IMPACT Chairman, Datuk Mohd Noor Amin & Symantec CTO, Mark Bergman
  - Session held at JW Marriot, Kuala Lumpur, December 2009
Cybersecurity Service Deployed
Training and Skills Development

- Management Track
  - Security Management
  - Security Audits
  - Policy and Legal Framework

- Technical Track
  - ISO 27001 Information Security Management (ISMS) Implementation
  - ISO 27001 Information Security Management System Lead Auditor (ISMS)
  - Cyber Crime: Domestic and International Models of Cooperation
  - Legal Responses to Emerging Cyber Crimes

- Network Security
  - Network Systems Security and Audits
  - Developing and Implementing Computer Incident Response Team (CIRT)
  - SCADA Security
  - Securing ISP Networks and Systems
  - Advanced Honeypots and Malware Collection
  - Network Forensics and Investigations
  - Host Forensics with Open Source Tools for Incident Response
  - Malware Analysis and Reverse Engineering
  - Application Security
  - Web Application Security
  - Law Enforcement
  - Network Investigation for Law Enforcement
1. IMPACT’s Centre for Global Response (GRC)

- Global platform for alerts, early warning and cooperation; emergency response to facilitate identification of cyberthreats and share information and resources to assist Member States in taking appropriate action.
  - Network Early Warning System (NEWS)
    - Collaboration with global industry partners
  - Electronically Secure Collaborative Application Platform for Experts (ESCAPE)
    - Key experts and personnel from partner countries (law enforcement, regulators, country focal, cybersecurity experts, etc)
2. IMPACT’s Centre for Training and Skills Development

- Scholarships for developing countries and organization of specific training workshops to facilitate knowledge sharing among cybersecurity community.
  - Specialized training programs
  - Specialized seminars & workshops
  - Trainings via ITU’s Centre of Excellence (CoE)
  - Scholarship programs – partnership with global certification bodies
    - SANS (US$1 mil grant)
    - EC-Council (US$1 mil grant)
    - Global certification courses
    - (ISC)²
3. IMPACT’s Centre for Security Assurance and Research

- Establishment of CIRT, charged with the responsibility of serving as a trusted, central coordination cybersecurity point of contact within a country, aimed at identifying, defending, responding to and managing cyberthreats.

  - Security Assurance
    IMPACT Government Security Scorecard (IGSS), CIRT-Lite (Computer Incident Response Team), Professional services (vulnerability assessment, security audits, etc.)

  - Research
    Facilitation & coordination of cybersecurity research through IMPACT Research Online Network (IRON)
4. IMPACT’s Centre for Policy and International Cooperation

- With the support of ITU, the Centre fosters international cooperation through specific programmes such as coordinated cyberdrill exercises between countries.
  - Policy: Harmonization of policies, policy advisory & best practices
    - World Cyber Security Summit
    - Panel of Policy Expert Advisors
  - International cooperation: Partner country coordination, partnership and collaboration with industry, academia & international organizations
IMPACT Awards

- IMPACT received double honours at (ISC)2’s annual Asia Pacific Information Security Leadership Achievements (ISLA) Program 2010 (Singapore, July 2010)

  - Senior Information Security Practitioner Award Honouree: 
    **Philip Victor – Director of Training, Skills Development & Outreach**
  - Information Security Practitioner Award Honouree: 
    **Sivanathan – Manager, GRC Professional Services**
The United Nations Chief Executive Board (CEB) the highest level coordination mechanism within UN, has given high priority to Cybersecurity, following a proposal from the ITU Secretary General, on a UN-wide strategy.

The CEB welcomed the GCA as a framework to be applied also within the UN, in order to deliver security services to UN agencies (for instance through the ITU IMPACT, and as a mechanism for Inter agency coordination.

ITU and UN ODC have been identified as lead UN bodies in cybersecurity and cybercrime.

The ITU Secretary General and UN ODC Executive Director agreed to establish formal collaboration, in accordance with the mandates ITU and UNODC for a harmonized UN-wide strategy for Cybersecurity and Cybercrime.
Conclusions

- Cybersecurity is a global issue and it requires a global response.
- ITU, as the sole Facilitator of WSIS Action Line C5, is in a unique position to promote international cooperation through its Global Cybersecurity Agenda (GCA) and the ITU-IMPACT’s endeavor which is the first truly global multi-stakeholder and public-private alliance against cyber threats.
- Cooperation and coordination between Member States, through United Nations is indispensable to reach consensus on global strategies and involve all relevant bodies and stakeholders.

“Only by joining forces and bringing together our strategic capabilities will we be able to address current and emerging cyberthreats!”
THANK YOU

For further information
www.itu.int/cybersecurity
(gca@itu.int)