



## SESSION BACKGROUND PAPER

---

3 November 2009  
Original: English

# Building Confidence and Security in the Use of ICTs *Background Paper – Panel 5*

## 1. BACKGROUND

Cyberspace continues to grow exponentially. The global total of Internet users has trebled since 2000 and is projected to reach 1.85 billion users by the end of 2009. The Internet is now an integral part of the global economy and social structure - individuals, entire industries and governments all rely on the Internet and Information and Communication Technologies (ICTs) for a wide variety of needs, including banking, power supply, emergency services, transportation, education and social networking, etc. However, such rapid growth in cyberspace has not been accompanied by an adequate increase in cybersecurity.

Cyberspace today is challenged by growth in security vulnerabilities that can endanger the whole economic and social system of a country. ICT users in every domain are at risk of many different kind of attacks, including identity theft, online fraud, spam, malware, Denial of Service (DoS) attacks, espionage, cyber-terrorism, information warfare and a growing number of other cyber-threats. Confidence and security in the use of ICTs are fundamental in building an inclusive, secure and global information society. Confidence and security in the use of ICTs are vital, as acknowledged by the World Summit on the Information Society (WSIS).

As clearly stated by WSIS texts <sup>1</sup>, *“a global culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies”*. However, due to the borderless and transnational nature of cyber-threats, this goal has not yet been achieved and attempts to address the legal, technical and institutional challenges relating to building confidence and security in the use of ICTs are often still inadequate at the national and regional levels.

## 2. PURPOSE OF THIS PAPER

This Background Paper aims to give an overview of the current developments in the cybersecurity field globally, as well as some specific information on trends within the CIS region. It aims to update readers on recent ITU activities in CIS countries and provides indications and recommendations on possible ways forward.

## 3. CURRENT SITUATION

Cyber-threats have evolved drastically since the first attempts were made to penetrate Information Technology systems thirty years ago. The evolution of ICTs has not only advanced greater computational power and miniaturization, with evident benefits for end-users, but also opened up greater opportunities for criminals to exploit ICTs for malicious purposes. Nowadays, cyber-threats have achieved greater

---

<sup>1</sup> Paragraph 35 – WSIS Geneva Declaration of Principles, 2003.

sophistication in terms of both efficiency and effectiveness. Distributed and automated virtual robots (e.g. botnets) are practically independent autonomous entities that, once activated, are able to execute a huge variety of attacks without human intervention, generating illegal revenues amounting to billions of dollars. Cybercrime is also on the rise. A 2007 study found that data theft and breaches from cyber-crime may have cost businesses as much as US\$1 trillion globally in lost intellectual property and expenditures for repairing cyber-related damage.<sup>2</sup>

The economic, social and political impact of such attacks can be enormous, generating massive losses in income and creating breaches in ICT systems used by countries to operate key public services. Attacks such as denial of service<sup>3</sup> have crashed the networks of companies like Yahoo!, eBay, Amazon, and others, costing them millions of dollars in lost business. The presence and prevalence of malicious viruses also continue to grow. The Conficker worm has been identified as the top menace in 2009 with regards to worms and viruses. Conficker A exploits a vulnerability in Microsoft Windows, generating a list of 250 random domains. Early in 2009, Conficker B appeared, which passes from computer to computer via network shares and USB devices. Conficker C shuts down security services (e.g. anti-virus software) and blocks security update websites. All three variations of the worm have infected some 15 million computers around the world. Conficker is just one example of a threat that may jeopardize the operations of an entire company's or government's network for hours, or even days.

Botnet<sup>4</sup>-related attacks have also risen massively over the past few years, evolving from small networks of a dozen PCs controlled from a single command and control center (C&C) into sophisticated distributed systems comprising millions of computers with decentralized control. Using the different methods of attacks (from denial-of-service, to theft of confidential information, spam, phishing<sup>5</sup> etc.), botnet-related attacks are now a key element of cybercriminals' strategies. On average, some 302,000 zombies were activated each day for the purpose of malicious activity worldwide within the first quarter of 2009.<sup>6</sup>

Social networking sites such as Facebook, Twitter and MySpace have also become targets for cybercriminals seeking illicit revenues by tricking computer users or by stealing passwords for access to personal and financial accounts. As these sites gain in popularity, the number, types and severity of phishing attacks have also risen. Overall, experience shows that web navigation is still one of the main means of infection. During Q1 2009, an analysis was carried out on the websites most likely to contain malware or phishing. Pornographic and sexually-explicit sites topped the list of sites infected with malware, but job search sites are also a source of potential infection. Criminal activity sites fell from first place in the last quarter of 2008 to sixth place in Q1 2009. On the list of web categories manipulated by phishing, download sites and social networks continue to fall victim to new schemes. Newcomers to the list include the number one category - health and medicine - plus chat-sites and web-based email.

---

<sup>2</sup> See McAfee Virtual Criminology Report at:

[http://www.mcafee.com/us/research/criminology\\_report/default.html](http://www.mcafee.com/us/research/criminology_report/default.html)

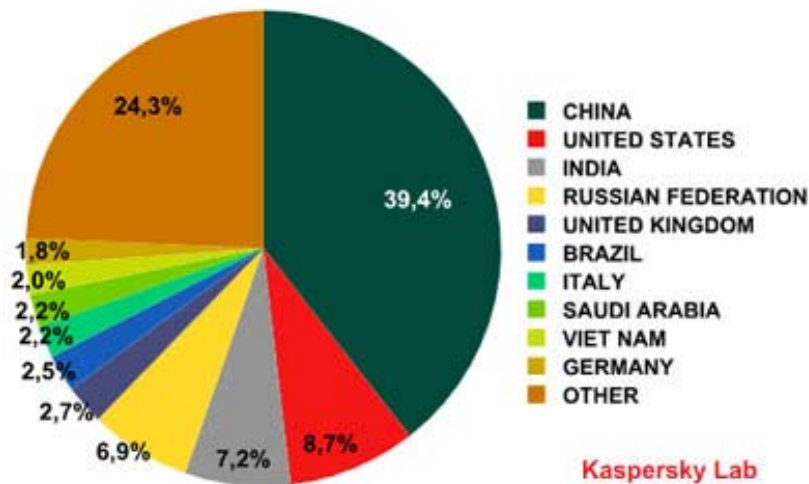
<sup>3</sup> A "denial-of-service" attack consists of preventing legitimate users of an ICT service from using that service.

<sup>4</sup> A botnet is a networked collection of computers infected with software that can be remotely controlled to awaken and perform some task.

<sup>5</sup> Phishing is the technique to acquire sensitive information (usernames, passwords, credit card details etc) by simulating a trustworthy entity (e.g. e-banking web site).

<sup>6</sup> Common Touch Software Online Lab.

Figure 1: Originating Countries with most attempts to infect computers via the web



Source: Kaspersky Lab.

Spam is also one of the most consolidated techniques to implement cyber-attacks. From their quick update of the half-year situation worldwide in mid-2009 (Source - Kaspersky Lab):

- The economic crisis has not impacted the volume of spam - spam averaged 85.5% of email traffic;
- Malicious attachments were found in 0.3% of messages;
- 0.6% of all messages contained links to phishing sites;
- Asian and Latin American countries became the main sources of spam, with a shift away from Western European countries, the United States and Russia;
- The amount of spam advertising small- and medium-sized businesses has declined during the recession.
- Spam advertising spammer services have partly replaced messages containing offers for concrete goods and services.

Apart from the IT-related aspects of cyber-threats, there are some other key elements to be taken into account:

- Lack of cybersecurity strategy at the national level can contribute strongly to a country's exposure to cyber-threats;
- Lack of solid legal frameworks specifically focused on combating cyber-crime could encourage criminal activities;
- Lack of dedicated organizational structures affiliated to governments could limit the operational and coordination capacity of a country to respond to cyber-attacks;
- Lack of mechanisms for international cooperation and coordination with recognized international and intergovernmental organizations could slow down the exchange of information and know-how necessary to build adequate capacity within a country.

All these above-mentioned elements should be addressed in a harmonized and integrated manner to ensure the consistency of the solutions adopted and compliance with the core principle of international cooperation, as called for by the WSIS.

ITU has been working hard to elaborate global strategies and related tools aimed at assisting Member States in fighting cyber-threats. Launched in 2007 by ITU Secretary-General, Dr. Hamadoun I. Touré, the ITU Global Cybersecurity Agenda (GCA)<sup>7</sup> is a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, seeking to encourage collaboration with and between all relevant partners and build on existing initiatives to avoid duplicating efforts. The GCA is now in its operational phase, and the ITU Telecommunication Development Bureau (BDT) is making available to all ITU Member States cybersecurity capabilities and tools that will provide a concrete solution to cyber-attacks and to achieve cybersecurity (see Annex).

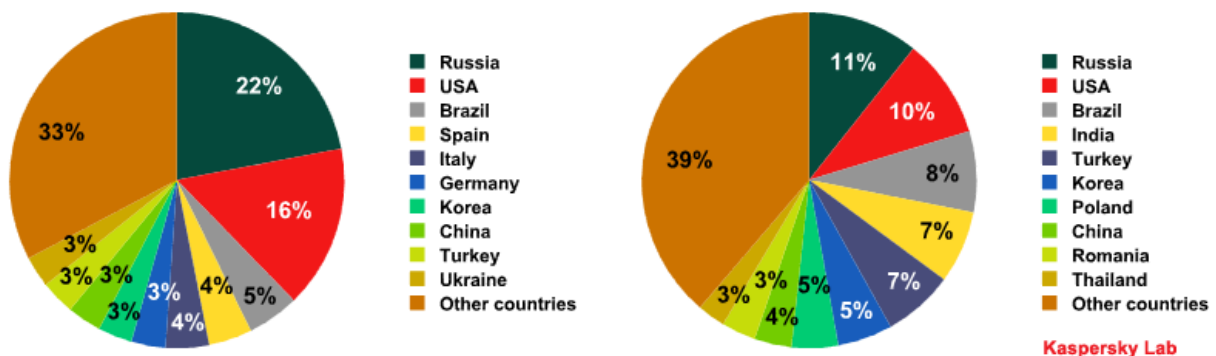
### 3.1 Situation in the CIS Region

The current situation in the CIS region reflects many of the trends above. The same trends identified at the global level can be applied within the region, including:

- Growing presence of attacks linked to web-surfing and social networking;
- Growing presence of botnets; and
- Stable, but consolidated presence of spam.

According to the Kaspersky Lab, “the top ten countries which are major sources of spam have changed considerably over the past six months. Less and less spam is coming from Spain and Italy, which previously took 3rd and 4th places, respectively. These countries are no longer in the top ten, with Germany and Ukraine also departing from the ranking. More spam now originates in India, Thailand, Romania, and Poland, all of which are now included in the top ten”.

Figure 2: Top ten sources of spam (2H 2008; 1H 2009)



Source: Kaspersky Lab.

Even if we are experiencing a shift towards the east in terms of spam generation, the CIS region is still at risk. One example is what happened in the Kyrgyz Republic at the beginning of 2009:

- Distributed Denial of Service (DDOS) attacks from Russian IPs disrupted the networks of the two largest ISPs in the country;
- Measuring the impact of the attack proved difficult, as security firms do not appear to have sensors within the nation’s networks, meaning that there are few reliable reports of bandwidth utilization.

<sup>7</sup> <http://www.itu.int/osg/csd/cybersecurity/gca/index.html>

This example emphasizes some of the main issues to be addressed in the cybersecurity field:

- Regional and international cooperation is key to addressing the borderless nature of cyber-threats;
- The establishment of sound organizational structures (such as monitoring systems, early warning systems, incident management capabilities) is key to responding quickly to cyber-threats;
- Prevention and response procedures and systems have to be complemented by the establishment of an over-arching policy framework and solid legal measures to ensure follow-up to the detection of cyber-threats and identification of cybercriminals.

In order to assess the needs at the regional level and to provide a platform to discuss cybersecurity-related issues, ITU organized a Regional Cybersecurity Forum for Europe and CIS<sup>8</sup> in Sofia, Bulgaria on 7-9 October 2008. The Forum, which was hosted by the State Agency for Information Technology and Communications (SAITC) of the Republic of Bulgaria, aimed to identify some of the main challenges faced by countries in Europe and CIS in developing frameworks for cybersecurity, to consider best practices, share information on cybersecurity development activities being undertaken by ITU as well as other entities, and review the role of various actors in promoting a culture of cybersecurity. The Forum also considered initiatives to increase cooperation and coordination amongst the different stakeholders, at the regional and international levels. Approximately 130 people from 25 countries participated in the event from Europe and CIS, as well as from other parts of the world.

During the event, a meeting was organized with the RCC Secretariat, to share views on possible regional approaches on cybersecurity. A presentation was made by ITU/BDT, which was later sent to all RCC Members through the RCC Secretariat. Initial work has been undertaken between ITU and representatives from the CIS region on cybersecurity and potential concrete opportunities to be identified and undertaken.

#### 4. Conclusions and Recommendations

The CIS region, in common with all other ITU regions, can promote cybersecurity by making use of regional and international cooperation strategies which, linked to national cybersecurity strategies, could constitute a huge leap towards building confidence and security in the use of ICTs. Concrete actions<sup>9</sup> and possible ways forward were already identified during the Regional Cybersecurity Forum for Europe and CIS. Some of these recommendations listed below can be undertaken immediately, and with the support of ITU:

- Review and, if necessary, revise or draft new legislation, to criminalize the misuse of ICTs, taking into account rapidly-evolving cyber-threats.
- Develop the necessary organizational structures to detect, manage and respond to cyber-attacks. Such structures can be affiliated directly with the Government or operating in close coordination with the Government. Some possible components of such a structure could include:
  - A national cybersecurity coordinator (an individual or an office) to organize the work and coordinate the efforts, interacting with Government, business and academia.
  - Incident management capabilities with national responsibility. This activity would involve the possible creation of a National Cybersecurity Center with the medium- to long-term objective of establishing a CERT/CSIRT.
- Inject measures that enhance the protection of children into the country's ongoing cybersecurity-related activities. This would involve technical mechanisms aimed at mitigating the risks for young people and children online, including:
  - Development of a framework for authentication and authorization to ensure that children are protected from inappropriate material.
  - Development of an internationally-recognized database for law enforcement agencies.

---

<sup>8</sup> <http://www.itu.int/ITU-D/cyb/events/2008/sofia/index.html>

<sup>9</sup> <http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sofia-cybersecurity-outputs-oct-08.pdf>

Using the ITU-IMPACT collaboration (see Annex for more details), ITU can make available immediately and free of charge a set of capabilities to promote cybersecurity to all CIS Member States, aimed at detecting, monitoring and activating the countermeasures necessary to properly respond to cyber-attacks to minimize damage and losses from cyber-attack. Furthermore, ITU can provide support and technical assistance in the process toward establishing and harmonizing at the regional level those legal measures that are required to complement and follow up the detection and identification of cybercriminals.

These actions will also take in consideration the specific requirements of users, with special attention to be given to children. ITU has established a Child Online Protection initiative<sup>10</sup> to address this issue, and countries in the CIS region could greatly benefit from this initiative.

---

<sup>10</sup> <http://www.itu.int/osg/csd/cybersecurity/gca/cop/>

**Annex**  
**Information Note on the ITU-IMPACT Collaboration**

**1. Background**

As the United Nations' lead agency for telecommunication and information technology, identified as lead moderator/facilitator of WSIS Action Line C5 "Building confidence and security in the use of ICTs", and within the framework of the Global Cybersecurity Agenda (GCA), the 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, together with ITU Member States and leading global partners from industry and academia.

IMPACT is the first global public-private initiative against cyber-threats. The initiative aims to bring together governments, industry leaders and cybersecurity experts in order to enhance the global community's capacity to prevent, defend and respond to cyber-threats.

On 3 September 2008, ITU and IMPACT formally entered into a Memorandum of Understanding (MoU) in which IMPACT's new state-of-the-art global headquarters in Cyberjaya, Malaysia, has effectively become the physical home of the GCA. Under this collaboration, ITU and IMPACT provide ITU's 191 member states with the expertise, facilities and resources to effectively address the world's most serious cyber-threats.

On March 20 2009, the global headquarters of IMPACT was inaugurated by Malaysia's Prime Minister Dato' Seri Abdullah Haji Ahmad Badawi and ITU Secretary-General Dr. Hamadoun Touré. Government ministers, industry leaders, technology luminaries and international cybersecurity experts from several countries were in attendance to chart the future course for IMPACT as a global multilateral platform facilitating the partnership between governments and the private sector in combating cyber-threats.

**2. Partners and Goals**

The GCA was launched by the ITU Secretary-General as the ITU framework for international multi-stakeholder cooperation towards a safer and more secure information society, and focuses on the following five work areas:

- Legal Measures;
- Technical and Procedural Measures;
- Organizational Structures;
- Capacity Building; and
- International Cooperation.

The foundation of IMPACT is built on the following key tracks:

- Centre for Global Response;
- Centre for Policy and International Cooperation;
- Centre for Training and Skills Development; and
- Centre for Security Assurance and Research.

In accordance with the signed MoU and the objective of establishing an international framework for collaboration, the ITU and IMPACT have agreed to cooperate in the following areas, mapping the GCA pillars against the tracks identified by IMPACT:

- *Legal Measures* – IMPACT's Centre for Policy and International Cooperation. Elaboration of strategies for the development of model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures;
- *Organizational Structures* – IMPACT's Centre for Security Assurance and Research. Elaboration of global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime;
- *Technical and Procedural Measures* – IMPACT's Centre for Global Response. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives;
- *Capacity building* – IMPACT's Centre for Training and Skills Development. Development of a global strategy to facilitate human and institutional capacity- building to enhance knowledge and know-how across sectors and in all the above-mentioned areas;
- *International Cooperation* - IMPACT's Centre for Policy and International Cooperation. Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

One of the key aspects of this collaboration is the participation of world leaders in the cybersecurity field. ITU and IMPACT are collaborating with industry and academia including Symantec Corporation, Kaspersky Lab, F-Secure Corporation, Trend Micro Inc., Microsoft Corporation, as well as with leading cybersecurity training institutions like The SANS™ Institute, EC-Council, The HoneyNet Project and (ISC)<sup>2</sup>.

### **3. Implementation**

The ITU Telecommunication Development Bureau (BDT) has taken the lead in facilitating the implementation process, communicating with the ITU Member States, assessing their needs and ensuring proper follow-up in coordination with IMPACT, which is providing the necessary technical support and expertise in order to deploy cybersecurity capabilities and related capacity-building.

In April 2009, the BDT Director wrote to all ITU Member States explaining the initiative and inviting Administrations to join, in order to benefit from the services provided by IMPACT. BDT is also coordinating internally with the other ITU bureaus to ensure that all relevant ITU work on cybersecurity can be made available and used within the framework of the collaboration with IMPACT.

While the long-term plan is to implement all areas of GCA, following the approach mentioned above, currently, the following activities have been identified and linked to the ITU-IMPACT deployment process:

#### **3.1. Technical measures**

IMPACT's Global Response Center (GRC) has been identified as a global platform for Early Warning System and cooperation. GRC acts as the foremost cyber-threat resource centre for the global community. It provides emergency response to facilitate the identification of cyber-threats and sharing of resources to assist Members States. The two prime highlights of GRC are NEWS (Network Early Warning System) and ESCAPE (Electronically Secure Collaboration Application Platform for Experts). NEWS can serve as a vehicle of information collaboration, as well as information dissemination of up-to-date information on the latest security trends. It provides features like:

- Real time threat monitoring and assessment, whereby member countries can see the global threat level and solutions to mitigate the threat;
- Statistical cyber-threat trend analysis, whereby member countries can view current cyber-trends and threats around the world, presented as a collection of easy-to-read charts, graphs, maps and tables;
- Malware threat centre, whereby members can upload malware and get feedback on the full technical details of malware analysis.

ESCAPE is a collaborative platform that enables authorized cyber-experts across the different countries to pool resources and remotely collaborate with each other in a secure and trusted environment.

This system features a comprehensive and growing database of key resources around the world – including IT experts, empowered persons (government officials) and other trusted bodies, who can be called in to assist during a crisis.

The Global Response Center has been identified as the initial service that will be made available free of charge - BDT is facilitating the deployment of the GRC to all Member States.

### **3.2. Organizational Structures and Watch and Warning Incident Response**

There is a clear understanding at the global level that dedicated structures within the country should be established to face and respond to cyber-attacks. Watch and warning systems and incident response activities, such as the establishment of Computer Incident Response Teams or CIRTs with national responsibility are essential in responding to such attacks.

One of the main functions of the CIRT is to serve as a trusted, central coordination point of contact for cybersecurity within a country, aimed at identifying, defending, responding and managing cyber-threats. They also play a key role in providing an information-sharing platform within the country, as well as addressing the transnational nature of cyber-threats, providing communication and coordination mechanisms at the international level.

In order to respond to the requests by several Member States in establishing such capability, ITU and IMPACT have elaborated a strategy for the implementation of national CIRTs, called *CIRTlite*. *CIRTlite* is being designed as a step-by-step phased approach, making available a framework that will allow Members States to adapt implementation according to the level of investment available and their requirements. The proposed solution (compliant with international best practices) would be integrated into the GRC, and will allow countries to be affiliated, if they wish, to [FIRST](#) (Forum of Incident Response and Security Teams).<sup>11</sup>

This phased approach will also allow further development and, most importantly, the possibility to trigger regional and international cooperation, as well as supporting the establishment of regional CIRTs.

BDT Programme 3 is in charge of the implementation aspects of the ITU-IMPACT collaboration and has established synergies with other BDT programmes and project (e.g. [EC Project](#))<sup>12</sup>, in order to harmonize the activities, specifically in the area of CIRT-related capacity-building as well as with the other ITU Bureaus. ITU would directly support countries in the implementation of national CIRTs through the establishment of an over-arching policy framework to support solutions and related watch, warning and incident response capabilities within a national strategy. Together with IMPACT, ITU will facilitate the deployment of the technical capabilities and the training that will be necessary to concretely establish national or regional CIRTs.

### **3.3. Capacity Building**

Any deployment of the capabilities mentioned above should be accompanied by capacity-building activities aimed at ensuring that the know-how required to operate them will be properly transferred. Existing ITU/BDT initiatives, such as the ITU National Cybersecurity/CIIP Self-Assessment Tool, the ITU Botnet Mitigation Toolkit, cybercrime legislation-related resources and the related training and capacity-building activities would be integrated into the ITU-IMPACT collaboration, in order to provide ITU Member States with a consolidated set of products and services.

IMPACT is coordinating with BDT to roll out the tools available through projects, training programmes and specific modules to be integrated into the GRC. Training and services to be offered include scholarships for developing countries and the organization of specific training workshops to facilitate knowledge-sharing.

---

<sup>11</sup> <http://www.first.org>

<sup>12</sup> [http://www.itu.int/ITU-D/projects/ITU\\_EC\\_ACP/](http://www.itu.int/ITU-D/projects/ITU_EC_ACP/)

IMPACT is building a catalogue of courses, according to the requirements specified by ITU, in order to respond to the training needs expressed by the countries.

#### ***4. Current Status of the Collaboration***

Following the BDT Director's invitation to the Administrations of all Member States, coordination has started with IMPACT and Member States. The collaboration status is up-to-date as of 8 September 2009.

- Thirty-eight countries have formally joined the ITU-IMPACT collaboration Afghanistan, Andorra, Brazil, Bulgaria, Burkina Faso, Cape Verde, Costa Rica, Côte d'Ivoire, Dem. Rep. of the Congo, Egypt, Gabon, Ghana, Kenya, India, Indonesia, Iraq, Israel, Italy, Lao P.D.R., Malaysia, Mauritius, Montenegro, Morocco, Nepal, Nigeria, Philippines, Poland, Serbia, Seychelles, Saudi Arabia, Switzerland, Syrian Arab Republic, Sudan, Tanzania, Tunisia, Uganda, United Arab Emirates and Zambia.
- By the end of year, all Member States that have confirmed their participation will be able to access the GRC. The deployment includes training sessions on the usage of the GRC and technical support services provided by IMPACT HQ to ensure further analysis in case of cyber-attacks.
- Twenty-two countries have established contact with ITU and IMPACT in response to the BDT Director's invitation: Austria, Australia, Bangladesh, Burundi, Cambodia, Czech Republic, Canada, France, Germany, Greece, Japan, Madagascar, Macedonia, Palestine, Romania, Rwanda, Singapore, South Africa, Spain, Turkey, Vietnam and Zimbabwe.
- Concerning the establishment of national and regional CIRTs, the African and European regions have been identified as the first regions to benefit from this assistance. In line also with the current developments of the ITU-EC project, ten countries from the African region have been identified: Burundi, Burkina Faso, Cote D'Ivoire, Ghana, Kenya, Nigeria, Rwanda, Tanzania, Uganda and Zambia; four countries, namely Czech Republic, Montenegro, Poland and Serbia, have been addressed for the European region. Coordination is underway with the Administrations, to finalize the process and organize the necessary resource mobilization to move to the operational phase.