



Office of the President of the Philippines
COMMISSION ON INFORMATION AND COMMUNICATIONS TECHNOLOGY

Message
H.E. Secretary Ray Anthony Roxas-Chua III
Chairman, Commission on Information and Communications Technology
Republic of the Philippines

**1st INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER-
TERRORISM (IMPACT)**
20-22 May 2008, Kuala Lumpur, Malaysia

Your excellencies, distinguished delegates, guests, ladies and gentlemen, a pleasant good morning to you all. It is a great honor and privilege to have been invited to participate as a panelist in this IMPACT World Cyber Security Summit. On behalf of the Philippine delegation and the Commission on Information and Communications Technology, or CICT, I would like to express our deepest gratitude to our gracious hosts from Malaysia who have been the epitome of hospitality and professionalism throughout this event. This is my first ever visit to Malaysia and from what I have seen so far, I am already looking forward to my next visit. I would also like to commend the Malaysian government for organizing this inaugural IMPACT World Cyber Security Summit. This forum comes at an opportune time and provides a venue for us to bring together our common interests and collaborative efforts to address the issue of cyber terrorism.

The Philippines itself is no stranger to cyber terrorism. In May 2000, the ILOVEYOU virus spread throughout the world infecting millions of computers and causing billions of dollars in damage globally. Subsequent investigations led to a Filipino programming student, who claimed that the release of the virus was purely accidental and that he meant no harm. If an innocent attempt at ingenuity can cause this much havoc, it is downright terrifying to imagine what people with malicious intent might be capable of.

The Philippine government affirms that cybercrime is an enduring problem in our increasingly technological society. We recognize that our infrastructures and processes are now heavily dependent on ICT and are therefore vulnerable to threats such as hacking, identity theft, spamming, phishing, denial-of-service attacks, malware, such as the ILOVEYOU virus, and probably the most disturbing, child pornography and cyber prostitution. Cybercrime is a persistent and growing threat, and we are one with the international community in recognizing the need to address this collectively. Let me now share with you some of the initiatives the Philippine government is undertaking to address this.

In 2005, our National Cyber Security Plan was approved by Her Excellency President Gloria Macapagal-Arroyo. This document now serves as the cornerstone of the Philippine information security policy. It is the instrument that guides us in the creation of a more secure and stable environment for the country's continued growth.

In general, our National Cyber Security Plan mandates the institutionalization of the necessary capabilities in the government and in the private sector to adequately meet and respond to challenges and threats against ICT infrastructures that are critical to the way of life and well-being of every Filipino.

In 2006, the CICT issued our Strategic Roadmap for the ICT Sector. The strategies and programs that are outlined in the ICT Roadmap flow from a carefully developed vision for the Philippines' ICT sector—to create a people-centered, inclusive and development-oriented information society that promotes sustainable development and improves the quality of life for Filipinos.

This ICT Roadmap is also a declaration of the Philippine government's belief in ICT as a critical tool for economic growth and development, and ultimately, for empowering the nation and citizens as individuals. By this document, the Philippine government reaffirms its commitment to provide equitable access to information and knowledge, and recognizes that ICT is the key to fulfilling this commitment to promote better governance, corporate performance, and individual achievement. Specifically, it states as one of its principles "a safe and trustworthy online environment for all."

We believe that cyber security is best addressed through coordination and collaboration among all stakeholders. In the Philippines, we have developed partnerships among the different government agencies, such as the CICT, Department of Justice, National Bureau of Investigation and Philippine National Police; private sector enterprises engaged in cyber security solutions; and non-government organizations such as the Information Systems Security Society of the Philippines, the Philippine Chapter of the Information Systems Audit and Control Association and the Philippine Computer Emergency Response Team, or PH-CERT. These partnerships are a clear manifestation of our collective concern for the development of a national cyber security strategy that addresses the needs of the country and its people.

I would like to highlight three areas that are of particular concern to the Philippine government when it comes to cyber security. First is the Philippines' large and growing mobile subscriber base. The Philippines is widely considered the text messaging capital of the world with 55 million mobile subscribers that sent an astonishing 1.4 billion text messages on New Year's Day alone.

Advances in technology have also allowed mobile subscribers to transfer prepaid credits from one mobile phone to another, thereby creating a new payment mechanism. Unfortunately, this has also made mobile phones the new target of cybercriminals. An increasing number of text-based scams have been victimizing unsuspecting mobile subscribers by promising monetary rewards in exchange for remitting a certain amount to a particular mobile number. These scams are particularly difficult to address, because the mobile subscribers in the Philippines are predominantly pre-paid subscribers who do not have to register their SIM cards with the telecom operators.

Incidentally, we would like to commend the APECTEL Security and Prosperity Steering Group chaired by Malaysia for supporting projects such as the “Handheld Mobile Device Security Workshop,” which will document best practices on securing mobile devices.

Second is the Philippines’ rapidly growing business process outsourcing, or BPO, industry, which includes call centers, back office, animation, medical and legal transcription, software development, engineering design and game development. The Philippines is considered a leading BPO destination with 300,000 IT-proficient workers that generated close to \$5 billion US dollars in export revenue in 2007. The Philippines was also named “Offshoring Destination of the Year” by the National Outsourcing Association of the UK and research firm IDC ranked Manila number 2 in its top 10 list of BPO destinations in the Asia-Pacific region, second only to Bangalore in India.

The CICT, in collaboration with the Business Processing Association of the Philippines, the umbrella organization of the BPO industry, is now establishing regional ICT hubs around the country. These hubs are being positioned to host BPO operators, aiming to increase job opportunities and boost the local economies in these areas. Currently, 24 cities around the country have been identified as ICT hubs and 16 of these already have a major BPO operator.

The importance of this high growth industry to the Philippine economy makes it crucial for us to protect our ICT infrastructure from various forms of cyber attacks. One major requirement of BPO customers is business continuity, so any downtime caused by cyber attacks will be very detrimental to BPO operators. In addition, BPO operators deal with highly sensitive corporate, medical and legal data on a daily basis, so the protection of such data and the infrastructure on which they are transmitted is of utmost importance.

Third is the area of child pornography and cyber prostitution. Given our population is predominantly Roman Catholic and approximately half the population is below the age of 21, we are very focused on protecting our women and children from online sexual predators. While cybercrimes such as online fraud and denial-of-service attacks could result in millions or even billions of dollars in damage, the damage caused by child pornography and cyber prostitution to innocent women and children far exceeds any monetary amount.

Recognizing that cyber security is a regional concern of Asia-Pacific economies, cyber security was taken up in a series of workshops during APECTEL35 held in Manila, Philippines. These workshops focused on malware and network security concerns covering banking, government financial institutions, insurance, transportation, power and telecom sectors, and facilitated discussions on the preparation of plans on the conduct of joint inter-agency responses to cyber threats and incidents. These workshops also opened doors for us to network with cyber security practitioners within APEC as well as its guests outside of the APEC region, such as the Council of Europe.

One important aspect of cyber security is the ability of every economy to respond to any cyber security related incidents in an expeditious manner. In this regard, it is imperative that economies conduct cyber security exercises on a periodic basis to ensure that our respective CERTs are able and ready to face various cyber security threats. We are in support of activities that enhance each country's CERT capability, including incidence drills and capacity building activities. We would like to commend Singapore for organizing the inaugural ASEAN CERT Incidence Drill, or ACID, in 2006 and Malaysia for recently organizing the APCERT Cyber Drill Exercise in 2007.

The Philippines, through the CICT's National Computer Center, also participates in international efforts related to eradicating spam, through the Seoul-Melbourne Anti-Spam Group. We are very glad to note the formation and continuing expansion of the Stop Spam Alliance, which initially includes the Seoul-Melbourne Anti-Spam Group and other associate partners, including the Asia-Pacific Telecommunity, or APT, and the Internet Society, or ISOC, to help coordinate international action against spam and related threats more effectively by gathering information and resources improving information sharing among participating entities.

I am proud to share that we have made significant strides in our cybercrime legislation over the past year. In October 2007, an International Conference on Cybercrime was held in Manila by the Department of Justice, the CICT and the Council of Europe, with the cooperation of Microsoft. We have since incorporated the feedback from the conference into our draft bill and submitted the revised draft to our legislators for review. Last month, we were invited by the Council of Europe to attend the "Octopus Interface Conference: Cooperation Against Cybercrime," where we were informed by the Council of Europe that the Philippines will be formally invited to accede to the Convention on Cybercrime.

While we have made good progress in our cybercrime legislation, we still have our work cut out for us. Our challenge now is convincing our legislators in Congress to prioritize ICT-related bills, such as the Anti-Cybercrime Bill. It is an uphill battle given the country's focus on more visible issues such as the rice shortage and rising oil prices, but I believe we have the passion, energy, and political will to see it through.

Your excellencies, the Philippines is not a technological powerhouse. We also do not have unlimited financial resources to throw at the problem. But Filipinos love technology and are quick to embrace it when it is affordable and it improves their way of life, so we feel it is our duty to contribute to this global effort. One thing the Philippine government can offer the world is our commitment—the commitment to fight cybercrime and to cooperate with other countries in doing so. I assure you we will continue to pour our efforts into putting the appropriate legal frameworks in place and we look forward to working with the international community in helping to ensure a world free from the threats of cyber terrorism.

Maraming salamat at mabuhay!