Cybersecurity work programme for developing countries

The integration of information and communication technologies (ICT) into almost every sphere of daily economic and social activity has increased the dependence of individuals, organizations and governments on globally interconnected networks. At the same time, new cyberthreats have emerged that have an impact on confidence and security in the use of ICT.

In order to protect networked infrastructure and address these threats, coordinated national action is required to prevent, respond to and recover from incidents. National frameworks and strategies are needed that allow stakeholders (end users, industry and governments) to use all the technical, legal and regulatory tools available to promote a culture of cybersecurity.

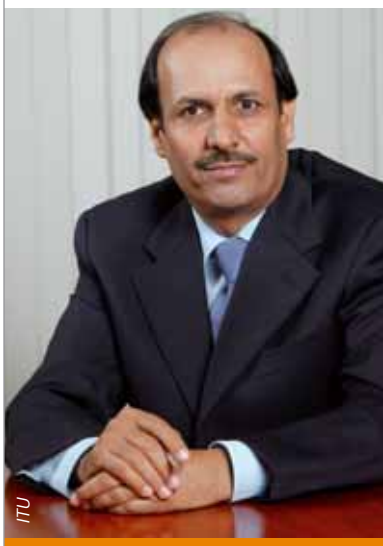
Among ITU Member States, while some are advanced in the formulation of national cybersecurity strategies, others are only just starting to consider the measures necessary to protect infrastructure that is now of fundamental social and economic importance. Developing countries with limited human, institutional and financial resources face particular challenges in formulating effective security policies. The *ITU Cybersecurity Work Programme for Developing Countries* sets out how the Telecommunication Development Sector (ITU–D) plans to assist those countries in practical ways during the 2007–2009 time-frame.

New toolkit to assess national cybersecurity

A toolkit is under development to assist governments to improve cybersecurity and formulate critical information infrastructure protection (CIIP) programmes. The *ITU National Cybersecurity/CIIP Readiness Self-Assessment Toolkit* examines necessary elements in formulating national security policies in an ever-changing ICT environment.

The draft toolkit is building upon work currently under way in ITU–D Study Group 1 on Question 22/1 "Securing information and communication networks: best practices for developing a culture of cybersecurity." The work includes a survey and raising awareness of:

- principal issues facing national policy-makers in working with stakeholders to build a culture of cybersecurity;
- principal sources of information and assistance;
- best practice employed by national policy-makers;
- unique challenges faced by developing countries and best practice for addressing them.


ITU

"Gaps in access to, and the use of, ICT do not only hinder countries' socio-economic development, but can also diminish the effectiveness of cooperation in building confidence and security in the use of ICT and promoting a global culture of cybersecurity. Our developing and least developed countries are increasingly at risk."

Sami Al Basheer Al Morshid
Director, ITU Telecommunication Development Bureau (BDT)

The purpose of this column "Cybersecurity Watch" is to share information on ITU activities and initiatives related to cybersecurity and countering spam. It is published once every quarter.
ITU welcomes contributions from its membership for publication in Cybersecurity Watch. For more information, contact

cybersecurity@itu.int

The toolkit aims to help governments better understand their existing systems, identify gaps that require attention, and prioritize national response efforts. It addresses political and management layers and necessary institutions, as well as relationships among government, industry and other private-sector entities.

The self-assessment toolkit is being designed to be used by government officials responsible for CIIP and formulating national cybersecurity policies. Input will be received from relevant ministries, as well as the private sector and other groups involved in promoting public awareness of a safer cyberspace. By using the toolkit, authorities will be provided with a snapshot of national policy, legislation and enforcement; institutions and institutional responsibility; personnel and expertise, and relationships among government entities and institutions.

As work progresses on the toolkit, information will be shared through the ITU–D website. Pilot country projects to test the toolkit are being run in conjunction with a number of workshops organized by ITU–D in cooperation with ITU Regional and Area Offices and the Telecommunication Standardization Sector (ITU–T).

The botnet battle

Botnets are networks of several thousand computers that have been infected with a virus which turns each of them into a "zombie" or "robot" without the owner's knowledge. This allows criminals to use the resulting collective computing power and aggregated Internet connectivity to perform tasks such as generating spam e-mails, launching distributed denial of service attacks (to blackmail companies, for example), destroying or amending data, and identity theft.

A growing underground economy has sprung up around botnet activities, involving authors of computer viruses or malware, controllers of botnets, and clients who commission illegal activity by renting botnets. These groups include organized crime gangs who communicate internationally through secure means such as restricted Internet Relay Chat channels. Stolen proceeds are transferred rapidly using online services to quickly move money between countries.

The problem is worldwide. However, emerging Internet economies are often particularly ill-equipped to deal with the catastrophic effects of botnets, resulting in a loss of confidence in the secure use of ICT.

ITU Botnet Mitigation Toolkit

ITU is developing a *Botnet Mitigation Toolkit* to assist developing countries in particular to deal with the growing problem of computers that are hijacked for criminal purposes. The toolkit draws on existing resources on the subject, identifies relevant local and international stakeholders, and takes into consideration the particular constraints of developing economies. The first edition of the toolkit will be made available to the ITU membership in December 2007.

The toolkit's aim is to combine government and grassroots initiatives, and to involve stakeholders to make best use of existing resources and infrastructure. It will incorporate the policy, technical and social aspects of mitigating the effects of botnets.

Policy aspects

In the policy domain, preventive measures involve setting up effective laws and regulations, as well as frameworks for efficient local and cross-border enforcement. Botnets often begin causing damage within minutes of being created, and the worst effects happen within the first 24 hours. Therefore, early detection is critical. However, this can only be done through a working system of responsible entities and contact points. The toolkit examines requirements for setting up such systems nationally and internationally.

Technical aspects

In the technical domain, alerts can be sent to public databases of Internet protocol (IP) assignment and routing, such as the autonomous system numbers (ASN) and IP "WHOIS" databases maintained by Regional Internet Registries such as APNIC for the Asia Pacific region, AFRINIC for Africa and LACNIC for Latin America. (WHOIS is a protocol used for querying a database to determine the owner of a domain name, an IP address or an autonomous system number on the Internet.)

However, Internet service providers (ISP), especially in developing economies, might not always update ASN and other information accurately to reflect the true and current state of their networks. In addition, larger ISPs might allocate smaller blocks of IP space to customer ISPs or other networks without simultaneously updating information, so that querying "who is the owner of the address" could show space owned by a large ISP, while the actual provider is a customer ISP, or even a customer of a customer. It is clear that developing countries need substantial investment in training to deal with such technical issues.

Social aspects

The effects of botnets (such as spam, phishing and malware) are often felt most by a public that lacks awareness of Internet safety. There is a need for sustained and widespread education campaigns, including resources available in local languages. When working on extending access to ICT to people who have no previous experience in this area, it is clearly essential to include the promotion of best practice in cybersecurity. As botnets are typically created through users inadvertently installing malware on their personal computers, mitigating botnet-related threats is no exception to this rule.

More information on ITU activities in the domain of cybersecurity can be found at:
www.itu.int/cybersecurity/

ITU–D's ICT Applications and Cybersecurity Division has information on its ongoing projects, resources and publications to assist ITU Member States, including an overview of the ITU Cybersecurity Work Programme for Developing Countries, as well as information on the toolkits mentioned in this article, at:
www.itu.int/ITU-D/cyb/

Details of related workshops and other events can be found at:
www.itu.int/ITU-D/cyb/events/