CYBERCRIME

The global challenge

UNODC
United Nations Office on Drugs and Crime

ITU

CYBERCRIME

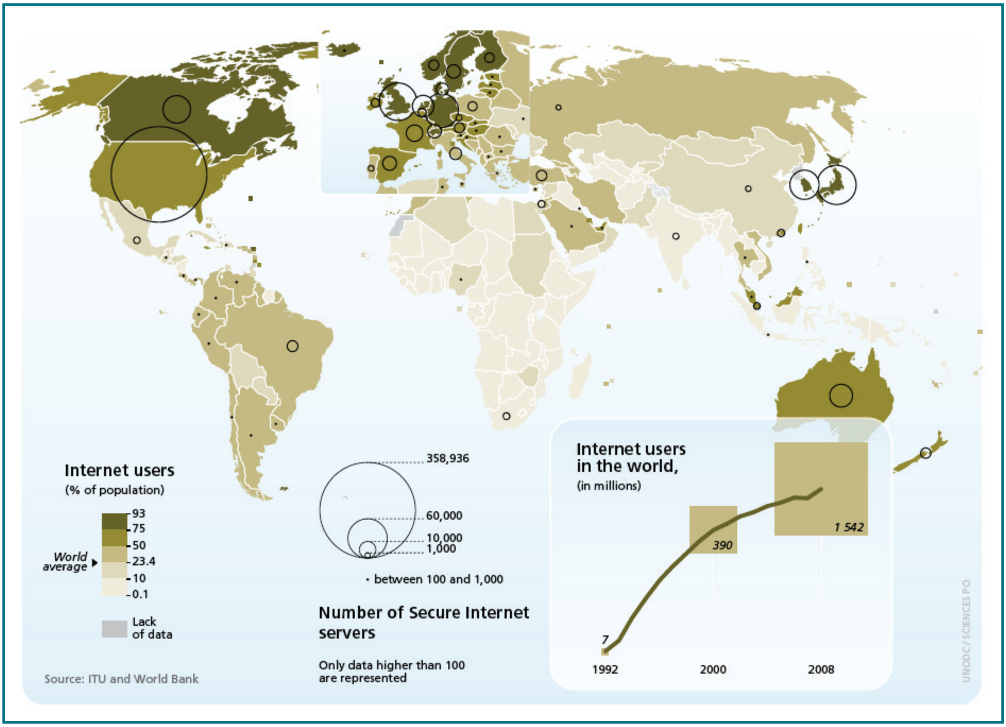
The global challenge

Cybercrime has developed from an ‘emerging crime’ to a serious manifestation of crime with great practical relevance

With the emerging use of computer technology, computer-related crime and cybercrime have become a significant global challenge. The ability to automate attacks against computer systems can lead, for example, to hundreds of thousands of registered attempts to interfere with, or illegally access, computer systems each day. Hundreds of new computer viruses are detected every month and virus toolkits enable computer users with even limited skills to create malicious software. Through networks of literally millions of compromised computer systems controlled by individual criminal groups, even the most powerful Internet services can be attacked. Such threats are expansive, not only in terms of quantity, but also in terms of quality. In recent years, the number of reports concerning targeted attacks against critical infrastructure have increased.

The Internet is based on single technical standards that allow global communication. This has the advantage of allowing the globalization of Internet services (such as Facebook, Google, Yahoo and others) that are operated in one country but can be accessed by users from all over the world. From a crime prevention perspective, however, it has the disadvantage that acts of cybercrime do not require that the offender by located in the same country as the victim. This explains why the vast majority of cybercrime offences have a transnational dimension. Successful prevention and combating of cybercrime therefore requires effective international cooperation through adequate legal instruments and well trained government and law enforcement personnel.

Although businesses in developed countries are often most affected by the abuse of Internet services to facilitate cybercrime, the topic is equally relevant for developing countries. Today there are more Internet users located in developing countries than in developed ones. In addition, the Internet offers small and medium enterprise, particularly, in small developing countries unique opportunities to connect with a global marketplace. In order to create both an enabling environment for enterprises and to protect users of Internet services in developing countries, it is necessary that countries have a clear legal framework and sufficient law enforcement and technological capacities in place to effectively fight cybercrime. Such frameworks and capacities are critical both to the protection of internet users within the country, and to the provision of effective support to foreign law enforcement agencies requesting international cooperation in cross-national cybercrime cases.



UNODC brings the experience of an organization that works globally in the area of crime prevention and criminal justice

The United Nations Office on Drugs and Crime (UNODC) is part of the United Nations Secretariat and a global leader in the fight against transnational crime. UNODC operates in all regions of the world through an extensive network of field offices. It offers countries in-depth expertise and a broad array of innovative services, tools and resources to counter various forms of criminal behaviour. This includes research and threat analysis, capacity development assistance, support in developing standards and norms, cross border cooperation and knowledge sharing, as well as communications and advocacy. In addition to significant work in the field of transnational crime and organized crime in general (especially in the context of the United Nations Convention against Transnational Organized Crime), UNODC addresses cybercrime through multiple channels. Over recent years, UNODC has received increasing mandates from the General Assembly, the Economic and Social Council, and the Commission on Crime Prevention and Criminal Justice to provide technical assistance and training to states to improve national legislation and to build the capacity of national authorities to prevent, detect, investigate and prosecute such crime in all its forms, including through enhancement of the security of computer networks. UNODC working groups and expert groups have provided in-depth analysis of the interface between crime and use of the Internet, including analysis of the involvement of international organizations in fighting cybercrime, terrorist use of the Internet, and identity-related crime. Pursuant to a mandate from the General Assembly, UNODC is currently engaged in a comprehensive study of the problem of cybercrime and responses to it. UNODC has published various handbooks and studies related to these topics and contributed to work on the prevention and combating of cybercrime carried out by other UN bodies and international/regional organizations.

ITU

International Telecommunications Union

ITU brings technical knowledge as well as tools and extensive experience in assisting developing countries to fight cybercrime

The International Telecommunication Union (ITU) is the United Nations specialized agency for information and communication technologies. It was founded on the principle of international cooperation between Member States and the private sector and today has a membership of 193 countries and over 700 sector members, from private sector research institutions and academia. This provides a unique platform to address cyberthreats and cybercrime since cybersecurity is a multidimensional issue, cutting across different sectors and stakeholders. ITU's mandate with regard to cybersecurity and cybercrime is based on decisions taken by the Membership during formal institutional gatherings, such as Plenipotentiary Conferences and world assemblies. In particular Plenipotentiary Resolution 130 (Rev. Guadalajara, 2010) strengthened the role of ITU on cybersecurity and cybercrime, instructing the Secretary General and the Directors of the ITU Bureaux on assisting Member States in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats.

Following the growing mandate given to the organization by Member States during the past years, ITU's concrete response – back in 2007 – was to launch the Global Cybersecurity Agenda, the 'GCA'. The GCA is a global framework for international cooperation aimed at enhancing global public confidence and security in the use of ICTs. The GCA follows a comprehensive approach towards a safer and more secure information society by going beyond legislation and international cooperation, and including technical and procedural measures as well as organizational structures. Legal and enforcement-related aspects of cybersecurity, including cybercrime, have been addressed in a number of study groups and within various regional conferences organized by the Development sector (ITU-D). Within an ITU/EU co-funded project, ITU is providing in-country assistance on improving legal frameworks addressing cybercrime as well as capacity building for various Asian, Caribbean and Pacific countries. The organization has also developed tools such as specific cybercrime training courses and related training materials for police, judges, lawyers and civil society. This includes a comprehensive publication on cybercrime that is made available free of charge in all UN languages.

5

UNODC-ITU MOU

Memorandum of Understanding

In May 2011, ITU and UNODC signed a Memorandum of Understanding. One of the key areas in which both organizations have decided to join efforts is capacity building. By uniting activities and combining their significant experience of in-country support, the two organizations can significantly expand the range of services and support for countries requesting assistance.

UNODC/ITU

offers:

- Combination of existing training material and courses, providing countries with wider access to a range of knowledge and tools
- Access to region-specific experience, through combination of two broad networks of field offices in all regions
- A comprehensive approach combining crime prevention, criminal justice and cybersecurity, covering all applicable legal and technical standards

6

SERVICES

How UNODC/ITU can support countries

UNODC/ITU offers individual support based on the requirements of the recipient country. Services range from support on specific issues (such as review of compliance with international and regional standards and best practices) to a full assessment and gap-analysis-based capacity building approach to the prevention and combating of cybercrime.

Assessment

UNODC/ITU can provide countries with assessment of institutional capacities and national normative frameworks applicable in the fight against cybercrime. Depending upon the nature of the request and the situation in the country concerned, such reviews can focus on specific aspects (e.g. the capacities of high tech crime units) or be carried out as a full review including all relevant areas of cybercrime prevention, investigation and prosecution.

Review of Legislation

UNODC/ITU can support countries in developing or strengthening cybercrime legislation. Such support can include identification of applicable provisions in existing legislation, comparative law analysis that compares existing legislation with international and regional best practices, as well as proposals for improvement of legislation through stakeholder consultations and support in legal drafting. UNODC/ITU legislation reviews are usually carried out by a team of local and international experts with the support of both headquarters and field offices.

Technical Assistance

UNODC/ITU provides a number of types of technical assistance. This can range from support in setting up institutional capacities to provision of equipment, software and training for law enforcement agencies. One of the strengths of the UNODC/ITU partnership in this regard is the availability of intensive cooperation with, and support from, industry players that frequently make computer-related tools available free of charge for developing countries.

Capacity Building

UNODC/ITU provides capacity building and training related to various aspects of cybercrime for different audiences and over a range of timescales. Training sessions can range from a two hour introductory presentation on the global or regional situation of cybercrime to a three week in-depth training course for law enforcement. Such training sessions cover legal as well as technical aspects of fighting cybercrime. UNODC/ITU also works closely with academic institutions that provide certified training and academic degree programs.

8 CONTACT

Requests for further information or support

For further information about the work of the UNODC/ITU in cybercrime, or concerning requests for support, please contact one of the two focal points for cybercrime:

UNODC

United Nations Office on Drugs and Crime
Attention: Gillian Murray, Chief, Focal Point for Cybercrime

Vienna International Centre, PO Box 500
A-1400 Vienna
Austria
Email: gillian.murray@unodc.org

ITU

International Telecommunications Union
Attention: Marco Obiso, Cybersecurity Coordinator

Place des Nations
CH-1211 Geneva 20
Switzerland
Email: marco.obiso@itu.int