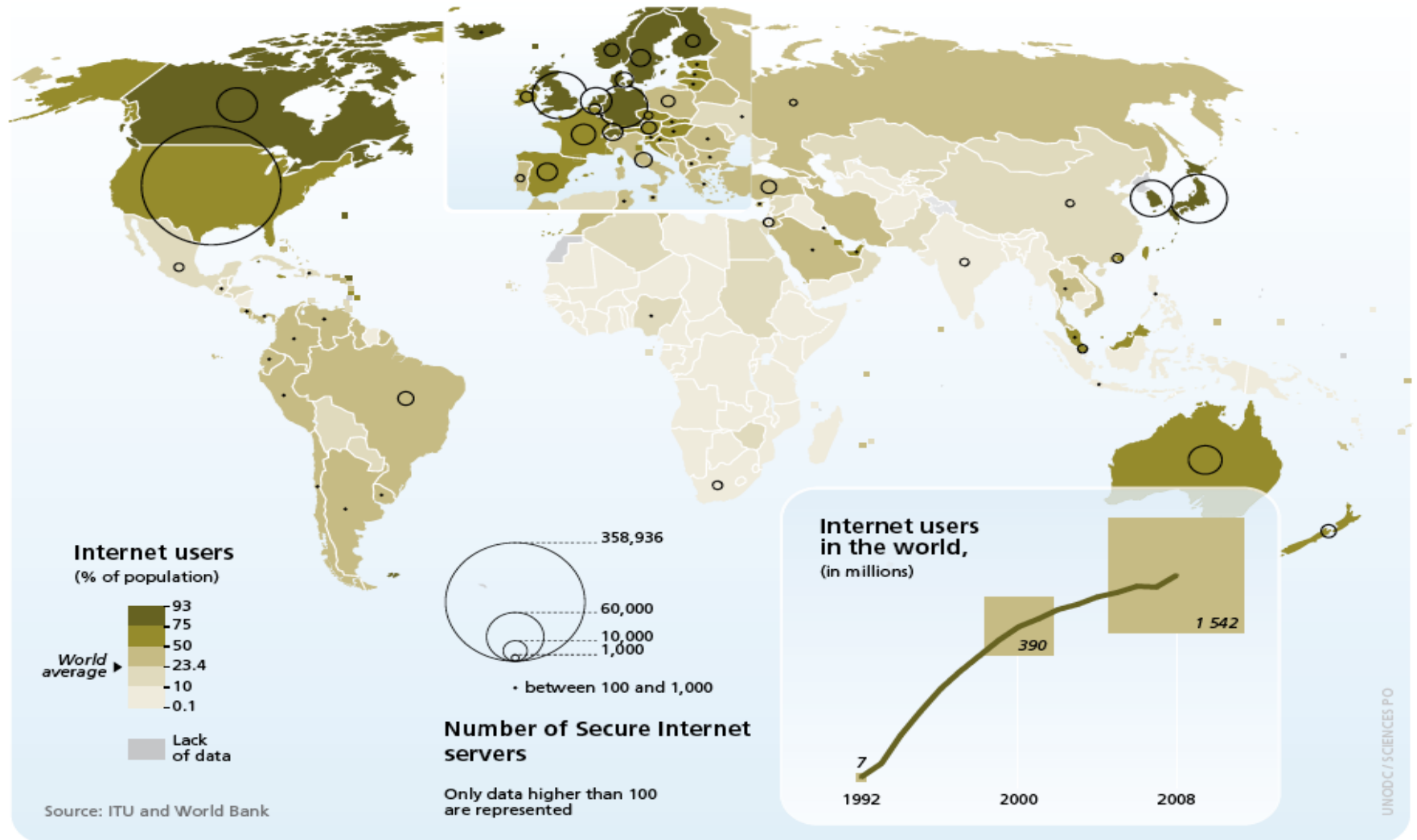


UNODC and the Global Response to Cybercrime

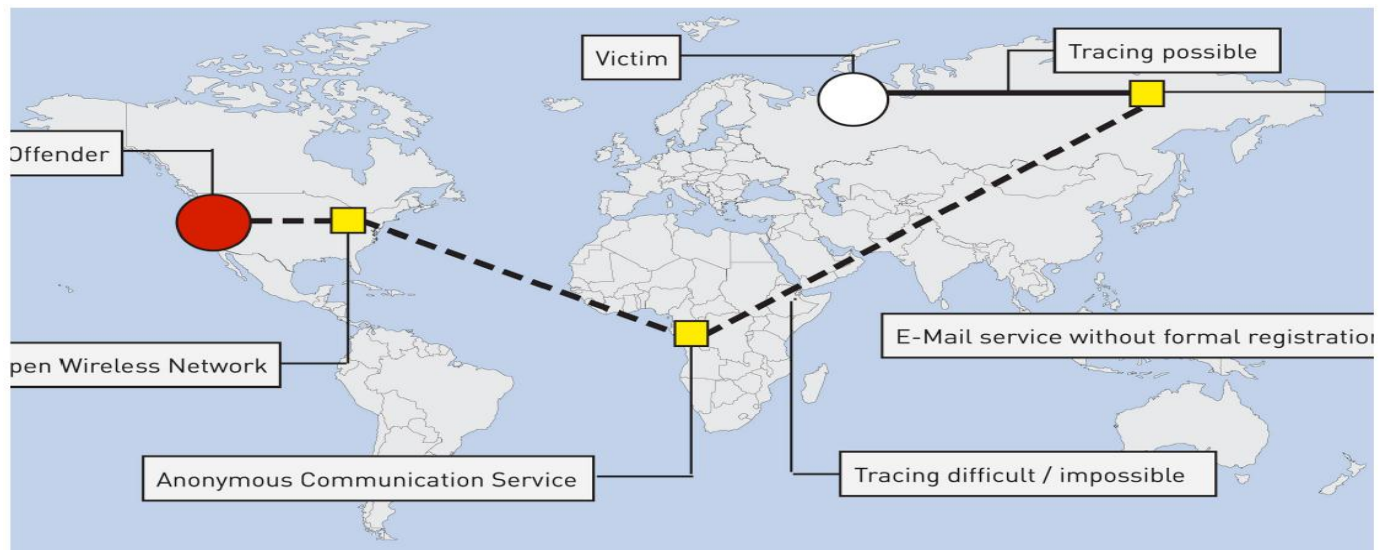
Organized Crime and Illicit Trafficking Branch
Division of Treaty Affairs

Cybercrime as a Global Challenge



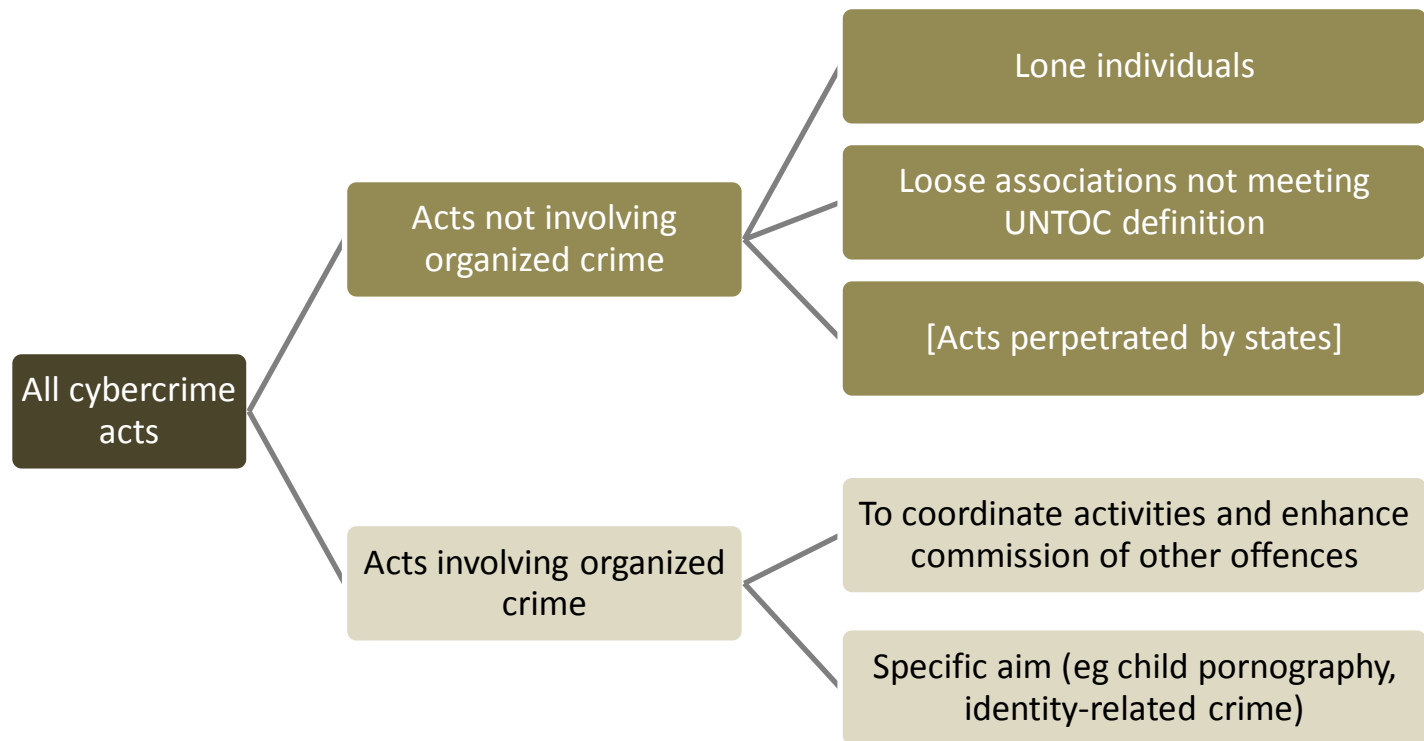
Transnational Dimension

- Transnational dimension due to underlying network architecture and global availability of services
- Essential to promote effective international cooperation in as close to real time as possible
- However, international cooperation only part of the solution. Also need technical solutions, education of users, legal measures and capacity building at national level



Links between Cybercrime and Organized Crime

- Definition of organized crime in the United Nations Convention against Transnational Organized Crime (UNTOC)
- Modalities of involvement of organized crime



UNODC Mandates in Cybercrime

- UN Convention against Transnational Organized Crime
 - (Art 3) Applicable to participation in an organized criminal group, laundering of proceeds of crime, and corruption, and also to any *serious* crime (defined as conduct punishable by a maximum deprivation of liberty of at least four years or a more serious penalty) where the offence is transnational in nature and involves an organized criminal group
- Recent Parliamentary Resolutions at the International Level
 - GA RES 64/211 – Creation of a Global Culture of Cybersecurity
 - GA RES 64/179 – Invites UNODC to explore ways and means of addressing emerging policy issues, including cybercrime
 - GA RES 65/230 – Requested the Commission on Crime Prevention and Criminal Justice to establish, in line with para 42 of the Salvador Declaration, an open-ended intergovernmental expert group on the problem of cybercrime and responses to it. Requested UNODC to build capacity of national authorities in order to deal with cybercrime (including the prevention, detection, investigation and prosecution of such crime, and to enhance the security of computer networks)
 - CCPCJ Res 20/8 – Reiterated need to strengthen cooperation with Member states and relevant organizations, including private sector, on combating cybercrime
 - ECOSOC Res 2011/33 – Requested UNODC to carry out a study on the effects of new information technologies on the abuse and exploitation of children and to assess training needs of States

UNODC Objectives

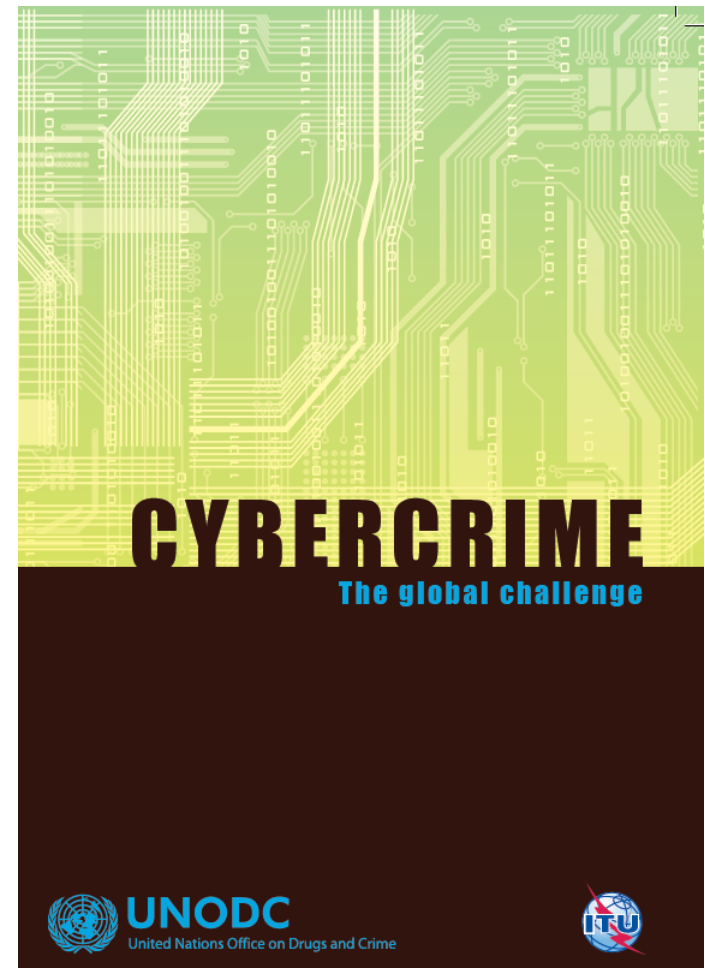
- Comparative advantage as only intergovernmental organization working on crime prevention and criminal justice at global level with specialized technical competence, operational capacity and long-term expertise in crime prevention, criminal justice and the rule of law
- Focus of efforts on developing countries through development of thematic programme
- Approach of using, building on, or adapting current good practice approaches
- Holistic approach covering criminal justice, prevention and awareness raising, regional and international cooperation and data collection, research and analysis
- Work through partnerships with other stakeholders including ITU, Interpol, OSCE, EU, Europol, Council of Europe, Member states, academia and private sector

UNODC Activities to Date

Development of training workshops on live data forensics (2009)	<ul style="list-style-type: none">Organized in cooperation with Irish Police Service and University College, Dublin
Development of handbook on identity-related crime (2009)	<ul style="list-style-type: none">Designed for use by legislators, policy-makers, prosecution and law enforcement authorities
Analysis of global cybercrime threat included in Transnational Organized Crime Threat Assessment (2010)	<ul style="list-style-type: none">Examined global threat of identity theft and child pornography
Establishment of joint activities with ITU (2011)	<ul style="list-style-type: none">Framework for UN response in areas of cybersecurity and cybercrime
Development of methodology for comprehensive cybercrime assessment (2011)	<ul style="list-style-type: none">Covering policy, legislation, regulation, investigation, prosecution, court, prevention and public-private partnerships
Pilot assessment mission (2011-2012)	<ul style="list-style-type: none">Cross-sectoral assessment mission
Development of questionnaire and desk research for comprehensive study (2011-2012)	<ul style="list-style-type: none">Questionnaire developed for Member states, private sector, intergovernmental organizations and academia

UNODC/ITU Global Activities

- Assessment
 - Of institutional capacities and national normative frameworks in the fight against cybercrime
- Review of Legislation
 - Including proposals for strengthening frameworks through stakeholder consultations and support to legal drafting
- Technical Assistance
 - Ranging from development of institutional capacities to provision of equipment, software and training for law enforcement agencies
- Capacity Building
 - Covering legal as well as technical aspects of combating cybercrime, delivered in cooperation with academic institutions



Cross-National Legal Frameworks

- To date, cybercrime primarily addressed through national legislation and cross-national frameworks (binding and non-binding), including Arab League Model Cyber Law, Commonwealth Model Law on Computer and Computer-related Crime, ECOWAS Directive, Council of Europe Convention on Cybercrime, EU Legislation
- Within preparatory meetings for the 11th Crime Congress in 2005 a number of Member States called for a UN Convention on Cybercrime but no decision to initiate such a process
- All four regional preparatory meetings of the 12th Crime Congress in 2010 called for the development of an international instrument. Member States decided to undertake a comprehensive study of the problem of cybercrime and responses to it

Comprehensive Study 2011-2013

The image displays three draft questionnaires for the Comprehensive Study 2011-2013, arranged horizontally. Each questionnaire is a document with a header, a title, and a body of text and tables.

- Left: Member State Questionnaire Draft September 2011**
 - Title:** MEMBER STATE QUESTIONNAIRE DRAFT SEPTEMBER 2011
 - Text:** This questionnaire is divided into fourteen tabs. Three are for completion by the legislative authority, three for completion by the police or law enforcement authorities, two for completion by prosecution authorities, two by court authorities, and three by the competent authority of authorities for international cooperation and technical assistance in the area of cybercrime.
 - Form:** Includes fields for Name of focal point, Institution, Address, Contact telephone number, Email address, and Email address of responsible officer.
 - Table:** A table with two columns: 'Act description' and 'Descriptions of terms used in the questionnaire'. It lists various acts and their descriptions.
- Middle: Private Sector Questionnaire Draft September 2011**
 - Title:** PRIVATE SECTOR QUESTIONNAIRE DRAFT SEPTEMBER 2011
 - Text:** This questionnaire is divided into two tabs. Each respondent should complete only one tab, depending upon the nature of the respondent organization. The first tab is for private sector organizations that consider themselves to be computer-related 'service providers'. This includes, for example, telephone companies, internet service providers (ISPs), website hosting providers, application service providers, storage service providers, software providers, e-commerce and online banking service providers, and computer security solution providers. Organizations in this category should complete the tab entitled 'Service Provider Respondent'. The second tab is for completion by all other organizations that do not consider themselves to be service providers. Such organizations should complete the tab entitled 'General Respondent'.
 - Form:** Includes fields for Name of respondent, Institution, Address, Contact telephone number, Email address, and Email address of responsible officer.
 - Table:** A table with two columns: 'Act description' and 'Descriptions of terms used in the questionnaire'. It lists various acts and their descriptions.
- Right: International Organization and Academic Institution Questionnaire Draft September 2011**
 - Title:** INTERNATIONAL ORGANIZATION and ACADEMIC INSTITUTION QUESTIONNAIRE DRAFT SEPTEMBER 2011
 - Text:** This questionnaire consists of just two tabs. The first tab (act descriptions) contains descriptions of terms used in the questionnaire. There are no questions for completion in the first tab. The second tab (Questionnaire) contains questions for completion related to research and statistics on cybercrime, technical assistance, and regulatory frameworks for preventing and combating cybercrime. The questions are applicable both to international organizations and to academic institutions.
 - Form:** Includes fields for Name of respondent, Institution, Address, Contact telephone number, Email address, and Email address of responsible officer.
 - Table:** A table with two columns: 'Act description' and 'Descriptions of terms used in the questionnaire'. It lists various acts and their descriptions.

Member state
questionnaire

Private sector
questionnaire

Intergovernmental
organizations and academia
questionnaire

Comprehensive study

Other
material and
consultations

Thank you

cybercrime@unodc.org