Cybercrime Questionnaire for Member States

General Assembly Resolution 65/230 (2010) requested the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration, an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, with a view to examining options to strengthen existing and to propose new national legal and international or other responses to cybercrime.

At its meeting held in Vienna from 17 to 21 January 2011, the open-ended intergovernmental expert group tasked UNODC with developing an instrument for collection of data based on thirteen topics identified by the expert group for inclusion in the study (UNODC/CCPCJ/EG.4/2011/2). This questionnaire is designed for completion by Member States. Questionnaires for completion by private sector entities, intergovernmental organizations and academia are administered separately.

Name of Focal Point (Coordinating Official):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

This questionnaire is divided into FOURTEEN TABS. Depending upon national structures, individual tabs may be completed by different authorities.

To coordinate the completion and return of the questionnaire, it is recommended that Member States appoint a single FOCAL POINT to act as a coordinating official for the questionnaire. FOCAL POINTS should consult the INSTRUCTIONS in TAB TWO of the questionnaire, and ensure that all respondents responsible for completing individual sections have access to and have read the instructions prior to completing the questionnaire.

The FOCAL POINT should ensure that all relevant tabs are completed by the appropriate authorities, collated, and returned as a single completed questionnaire by 31 May 2012. Instructions for submission of the completed questionnaire by file upload to UNODC's website are available at: www.unodc.org/cybercrime-study

Assistance with the completion of this questionnaire may be requested from:
UNODC, Conference Support Section, Organized Crime and Illicit Trafficking Branch
email: cybercrime@unodc.org

Introduction

INSTRUCTIONS

This questionnaire is divided into FOURTEEN TABS. Tabs ONE to THREE contain information only and are NOT for completion. Tab FOUR contains general questions. Tabs FIVE and SIX contain questions about legislation. Tabs SEVEN and EIGHT contain questions on police and law enforcement. Tabs NINE to TEN contain questions related to prosecution. Tab ELEVEN contains questions on courts. Tabs TWELVE to FOURTEEN contain questions on forms of international cooperation - extradition, mutual legal assistance, and technical assistance.

The FOCAL POINT coordinating this survey should identify an appropriate respondent for each tab. As requested by the focal point, please fill in the relevent tabs and return them, together with any attachments requested to the focal point. The FOCAL POINT is responsible for collation of all parts of the questionnaire and ensuring that the questionnaire with all completed tabs is uploaded to UNODC's website as a SINGLE EXCEL file. Requested attachments should be submitted in .PDF format.

Due to the features described below, the questionnaire should be completed ON SCREEN, saved electronically, and uploaded as a single Excel file. The questionnaire may be printed for reference, although it CANNOT be submitted in printed form.

Sections for information only			
Tab	Title	Information for FOCAL POINT and ALL Subject Matter Respondents	
1	Introduction	Authorization, purpose, and goals of questionnaire	
2	Instructions	Explanation of Excel-based questionnaire	
3	Act Descriptions	Descriptions of acts (offences) to be used in completion of questionnaire	
Sections for completion and return			
Tab	Title	Information Requested	Question numbers for attachments and web links
4	General Section	Strategies, Public-Private Partnerships, Resources	1, 7, 8, 10
5	Legislation I	Legislation, Jurisdiction, Freedoms and Restrictions	12
6	Legislation II	Criminal and Procedural Laws	
7	Police I	Offenses and Persons, Trends and Threats	
8	Police II	Investigations/Evidence, Practice, Capacity	
9	Prosecution I	Offenses and Persons, Trends and Threats	
10	Prosecution II	Evidence, Practice, Capacity	
11	Court I	Processing and Conviction, Practices, Capacity	185
12	Extradition	Authority, Processing, Mechanisms, Requests	193
13	Mutual Legal Assistance	Authority, Processing, Mechanisms, Requests	216
14	Technical Assistance	Technical Assistance Received and Delivered	

When EXCEL asks if MACROS should be enabled, please select YES in order to enable questionnaire features that are necessary to complete the questionnaire.

Comments to aid completion of the questionnaire are embedded in cells marked with a red triangle in the top right corner. Many cells in the questionnaire have drop down menus that allow users to select from among a range of options. These listed options are designated by solid blue outlines around the relevant answer box. Some cells allow multiple responses, others allow only one response. To display and scroll the listed options, click on the cell, then click on the arrow that appears to the right. To change an answer in the drop-down list selection, you may use the Backspace or Delete key to clear the cell and to select the appropriate answer choice. To select multiple options, click on each response you wish to select; use the Backspace or Delete key to eliminate or correct a response.

Many cells in the questionnaire request free text information and narratives. These cells may not appear to have enough space to record your entire answer on the screen, although they will accept a very large number of characters. All information entered and submitted will be transferred to the study database.

If information is unavailable, please leave the cell blank. Please do not enter 'n/a' or other response.

This section contains descriptions of key concepts and cybercrime acts to be used in the completion of this questionnaire.

For the purposes of this questionnaire only, the following terms shall have the following meanings:

Computer System	Refers to an electronic device or a group of inter-connected or related devices, including the Internet, one or more of which, can perform automated processing of computer data or other logical operations following a computer program. In addition to home desktop computers and laptop computers, this may include cell phones, smart phones, internet and wireless routers, external storage devices, and other devices designed to process computer data.
Computer Data	Refers to any representation of facts, concepts, information (including text, sound and images), and machine-readable code or instructions, that are in a form suitable for processing in a computer system, including a computer program that is capable of causing a computer system to perform a defined function. Computer data may be stored by the computer system in (temporary) memory, in (semi-permanent) solid state storage, or on a computer system hard disk or other magnetic or optical media.
Service Provider	Refers to any public or private entity that provides to users of its service the ability to communicate by means of a computer system, as well as any other entity that processes or stores computer data on behalf of such communication service or users of such service. This is the case, for example, for telephone companies, internet access providers, website hosting providers, storage service providers, and application service providers.

For the purposes of this questionnaire only, cybercrime acts include but are not limited to:

Acts against the confidentiality, integrity and availability of computer data and systems	
Illegal access to a computer system	Refers to acts involving entry into parts or the whole of a computer system without authorization or justification. This is the case, for example, if a perpetrator circumvents a firewall and enters the computer system of (for instance) a bank. This may also be the case if a user continues to remain connected to a computer system beyond his or her authorized time, such as when a perpetrator books server capacities for a certain period of time but continues to use them after the period has expired. Some national approaches require that the perpetrator circumvents protection measures or acts with specific intent.
Illegal access, interception or acquisition of computer data	Refers to acts involving gaining access to computer data without authorization or justification, including obtaining data during a transmission process that is not intended to be public, as well as obtaining computer data (such as by copying data) without authorization. This is the case, for example, if a perpetrator illegally accesses a computer database, records transmissions without right within a wireless network, or if a perpetrator, who is working for a particular company, copies files to take with him without authorization. Some national approaches require that the relevant data was protected against unauthorized access. Some national approaches also include the interception of electromagnetic emissions that may not be categorized as computer data. Industrial or corporate espionage may often involve the act of illegal access, interception or acquisition of computer data.
Illegal data interference or system interference	Refers to acts hindering the functioning of a computer system, as well as to acts involving damage, deletion, deterioration, alteration or suppression of computer data without authorization or justification. This is the case, for example, if a perpetrator submits so many requests to a computer system that it can no longer respond to legitimate requests (a so-called 'denial-of-service attack'), deletes computer program files necessary for the functioning of an internet server, or alters records in a computer database. Some national approaches cover only data-related acts whereas others also cover hardware manipulations. ‘Hacking’ into computer systems associated with critical infrastructure (such as water or electricity supply systems) may result in illegal data interference or system damage.

Production, distribution, or possession of computer misuse tools	Refers to acts involving the development or distribution of hardware or software solutions that can be used to carry out computer or internet-related offences. This is the case, for example, if a perpetrator develops a software tool to automate denial-of-service attacks. In order to avoid interference with the legitimate use of such tools (such as by security experts), some national approaches require that the tool is exclusively designed for illegal purposes, or that a perpetrator acts with the intention to use the tool to commit a crime.
Breach of privacy or data protection measures	Refers to acts involving the use of a computer system to process, disseminate, obtain, or access personal information in violation of data protection provisions. This is the case, for example, if a perpetrator operates an e-commerce business and discloses personal information from his customer database that he was required to keep confidential.

Computer-related acts for personal or financial gain	
Computer-related fraud or forgery	Refers to acts involving interference with or illegal accesses to a computer system or data with the intent of deceitfully or dishonestly obtaining money, other economic benefit or evading a liability, as well as to acts involving interference with a computer system or data in way those results in the creation of inauthentic computer data. This is the case, for example, if a perpetrator modifies the software used by a bank to redirect money transfer processes to his own account, or if a perpetrator modifies an authentic email from a financial institution with an underlying intent to defraud. Sending many such messages in an attempt to obtain personal information or to defraud is also referred to as 'phishing'. With respect to computer-related forgery, some national approaches require that the original computer data relate to documentation intended to create binding legal obligations. Others require only that a perpetrator intends the resultant modified version to be considered as or acted upon with respect to legal obligations.
Computer-related identity offences	Refers to acts involving the transfer, possession, or use, of means of identification of another person stored in computer data, without right, with the intent to commit, aid or abet any unlawful criminal activity. This is the case, for example, if a perpetrator, without right, obtains driving licence information from a computer system and either sells such data or uses it to hide his true identity when committing a crime. Some national approaches limit the application of such provisions to certain identification instruments.
Computer-related copyright and trademark offences	Refers to acts involving the copying of material stored in computer data or generates computer data in violation of copyright or trademark protections. This can be the case, for example, if a perpetrator distributes a song protected by copyright through a file-sharing system without the licence of the copyright owner.
Sending or controlling sending of SPAM	Refers to acts involving the use of a computer system to send out messages to a large number of recipients without authorization or request. In order to avoid an interference with regular business to customer communications, some national approaches require that a perpetrator provides false header information in such messages.

Specific computer-related acts	
Computer-related acts causing personal harm	Refers to acts involving the use of a computer system to harass, bully, threaten, stalk, or to cause fear in or intimidation of an individual. This is the case, for example, if a perpetrator sends insulting, threatening, offensive or abusive messages or images (also referred to as 'trolling'), or uses a computer system to track, stalk, or otherwise monitor or interfere with an individual's emotional or physical well-being. Acts solely constituting defamation are excluded from this category.
Computer-related acts involving racism or xenophobia	Refers to acts involving the use of a computer system to distribute or to make available racist and xenophobic material, or to threaten or insult an individual or group of persons for racist or xenophobic reasons. Racist and xenophobic material means any written material, image or other representation of ideas or theories which advocates, promotes or incites hatred, discrimination or violence against any individual or group of persons, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

Computer-related production, distribution, or possession of child pornography	Refers to acts involving the use of a computer system to produce, create, distribute, access or view, receive, store or possess any representation, by whatever means, of any real or fictional person under 18 years of age, or appearing to be under 18 years of age, engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. This is the case, for example, if a perpetrator downloads a digital picture showing the sexual abuse of a child.
Computer-related solicitation or 'grooming' of children	Refers to acts involving the use of a computer system, to propose to a child who has not reached the age of sexual consent to meet, for the purpose of committing a sex-related crime. This is the case, for example, if a perpetrator enters an internet chat with a child, pretends that he is also a child, and proposes to the child to meet, with the intention of abusing the child. This conduct may also be termed 'grooming'. Some national approaches may limit the offence to solicitation that is followed by a material act leading to a meeting.
Computer-related acts in support of terrorism offences	Refers to acts involving the use of a computer system in support of terrorism offences. This includes the use of a computer system to communicate a message to the public, with the intent to incite the commission of a terrorist offence or offences, where such conduct, whether or not directly advocating terrorist offences, presents a danger that one or more such offences may be committed (computer-related 'incitement to terrorism'). This also includes the use of a computer system to provide or collect funds with the intention that they should be used, or in the knowledge that they are to be used, in full or in part, in order to commit a terrorist offence or offences (computer-related 'terrorist financing offences'). This also includes the use of a computer system for the planning, research, preparation, or organization of a terrorist offence or offences (computer-related 'terrorist planning offences'). A terrorist offence means any act established in accordance with the universal legal instruments against terrorism, or otherwise intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities of a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act.

Name of Respondent (General Section):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

This section contains general questions regarding your country's national cybercrime strategy and coordinating agencies, national cybercrime priorities, challenges, and best practices, as well as the general availability of estimates and information on cybercrime.

National cybercrime priorities

			If YES
1	Does your country have a NATIONAL STRATEGY (or equivalent) on cybercrime?		Please ATTACH a copy or provide a direct WEB LINK to the full text of the instrument
			Which of the following areas does your country's NATIONAL STRATEGY address?

			If YES
2	In your country, is there a LEAD government INSTITUTION responsible for coordinating the prevention and combating of cybercrime?		Please identify the LEAD government INSTITUTION and briefly explain its role

		INSTITUTION	ROLE
3	Please identify OTHER GOVERNMENT INSTITUTIONS involved in the prevention and combating of cybercrime, and briefly specify their role.		

4 **Please identify NATIONAL PRIORITIES with respect to CYBERCRIME in each of the following areas, whether or not your country has a national cybercrime strategy:**

Prevention of Cybercrime	
Cybercrime Legislation	
Law Enforcement Investigation Capacity	
Criminal Justice Capacity to Prosecute	
Public Private Partnerships	
International Cooperation	
Other (Please specify)	

5 **What are the OVERALL national CHALLENGES and GOOD PRACTICES in your country with respect to cybercrime prevention and combating in the following areas?**

	Most significant CHALLENGE faced	GOOD PRACTICE for addressing the challenge
Prevention of Cybercrime		
Cybercrime Legislation		
Law Enforcement Investigation Capacity		
Criminal Justice Capacity to Prosecute		

Public Private Partnerships		
International Cooperation		
Other (Please specify)		

Public-private cooperation and prevention of cybercrime

		If YES
6 Do PUBLIC-PRIVATE PARTNERSHIPS exist for prevention and combating of cybercrime?		Please specify the following partnership elements
	The PARTNERS in the partnership	
	The SCOPE of the partnership	
	INFORMATION that is EXCHANGED as a result of the partnership	
	The BASIS of the partnership	

		If YES
		Please ATTACH a copy OR provide a direct WEB LINK to the full text of the instrument
7 Do national law or policy establish the ROLES and RESPONSIBILITIES of the PRIVATE SECTOR with respect to cybercrime?		
		Please summarize the MAIN ELEMENTS of the law or policy

		If NO
		Please describe how the ROLES and RESPONSIBILITIES of the PRIVATE SECTOR with respect to cybercrime are defined in your country
		If YES
		Please specify the relevant LAW or POLICY and either ATTACH a copy or provide a direct WEB LINK to the full text of the instrument
8	**Do national LEGISLATION or POLICY set out steps to be taken for the PREVENTION of cybercrime?**	
		Please describe the MAIN ELEMENTS of the LAW or POLICY

9	**Please describe any recent specific CYBERCRIME PREVENTION or AWARENESS activities or intitiatives undertaken by any of the following institutions:**	
	Law Enforcement Agencies	
	Other Government Institutions (please specify)	
	Non-Governmental Organizations or Academia	
	Private Sector Organizations	
	Other (Please specify)	

Information resources on cybercrime

			If YES: Please ATTACH a copy of the relevant report(s) OR provide a direct WEB LINK to the full text
10	Are statistics, reports, or other information available on the NATURE and EXTENT of cybercrime acts or the RESPONSE to it in your country from any of the following sources?	General population based survey	
		Survey of private companies	
		Expert assessment	
		Report of coordinating cybercrime commission or committee	
		Computer emergency response teams (CERTs) or computer security incident response teams (CSIRTs)	
		Report of IT security provider	
		Other (Please specify)	

Options for international legal or other responses to cybercrime

11	Please describe OPTIONS that should be considered to STRENGTHEN existing or to propose NEW INTERNATIONAL legal or other responses to CYBERCRIME.	

Name of Respondent (Legislation):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

Effective legislation is an essential component in the prevention and combating of cybercrime. This legislation section asks for the identification of relevant cybercrime laws, as well as containing questions on cross-national instruments, jurisdiction, and fundamental freedoms and rights within the framework of general principles of international and relevant domestic law, including privacy and data protection issues.

National cybercrime Laws

		Please provide the NAME (and ARTICLE number(s) if relevant) of the CYBER-SPECIFIC legislation	Please indicate the CYBERCRIME issues covered by the legislation	Please ATTACH a copy of the legislation or provide a direct WEB LINK to the full text of the legislation	What cross-national instruments were used to develop the legislation?
12	Please identify the main LEGISLATION that is SPECIFIC to CYBERCRIME in your country.				

13	Please specify any other additional relevant LEGISLATION or COMMENTS	

14	Are there plans to pass NEW LEGISLATION or to AMEND existing legislation on cybercrime?	

If YES			
Please provide the NAME of the NEW legislation or PLANNED amendments	Please indicate the EXPECTED YEAR of the NEW legislation or PLANNED amendments	Please indicate the CYBERCRIME issues to be covered by the NEW legislation or PLANNED amendments	What cross-national instruments will be used to draft or develop the NEW legislation or PLANNED amendments?

15	What is the most accurate CLASSIFICATION of your country's NATIONAL LEGAL SYSTEM?	CLASSIFICATION of legal system	If MIXED or OTHER legal system, please describe the main ELEMENTS of your legal system

Cross-national instruments and legal harmonization

		APPROACHES used to maintain NATIONAL legal traditions while incorporating cross-national instruments	SUCCESSES achieved in harmonization with cross-national instruments	LIMITATIONS encountered in harmonization with cross-national instruments
16	Where CROSS-NATIONAL instruments have been used as a basis of introducing or amending national legislation, please describe:			

		Other COUNTRIES in your REGION	Other COUNTRIES that are important to your country for the purposes of INTERNATIONAL COOPERATION	CROSS-NATIONAL CYBERCRIME INSTRUMENTS that are important to your country
17	To what extent do you consider that cybercrime LEGISLATION in your country is HARMONIZED with the following:			

Jurisdiction in cybercrime cases

			Cybercrime acts committed OUTSIDE of your country but which include EFFECTS or victims WITHIN your country	Cybercrime acts committed ENTIRELY OUTSIDE of your country
18	Please briefly describe the CRITERIA in NATIONAL LAW for:	CRIMINALIZATION of cybercrime acts committed outside of the country		
		PROSECUTION of such acts in the COURTS of your country		
		RESOLVING CONFLICTS OF		

	JURISDICTION, such as when two countries investigate and prosecute the same individuals for cybercrime acts committed outside of their respective countries		

19	Does your NATIONAL law provide a SUFFICIENT framework for the CRIMINALIZATION and PROSECUTION of cybercrime acts COMMITTED OUTSIDE of your country?		If YES Please describe the particular STRENGTHS and GOOD PRACTICE of your NATIONAL law
			If NO or IN PART Please describe the MAIN GAPS in your NATIONAL law

Fundamental freedoms within international and domestic law

	Freedom of Expression	
20	Please describe how law in your country protects FREEDOM OF EXPRESSION in ELECTRONIC form. Please specify relevant legislation references and/or rulings.	
	Please specify whether, and under what circumstances, FREEDOM OF EXPRESSION may be RESTRICTED for the purposes of preventing or combating cybercrime.	

	Protection of Privacy	
21	Please describe how law PROTECTS PRIVACY in the context of COMPUTER DATA or ELECTRONIC COMMUNICATION. Please specify relevant legislation references and/or rulings.	
	Please specify HOW PRIVACY RIGHTS function as SAFEGUARDS during police cybercrime investigations.	
	Please specify whether, and under what specific circumstances, PRIVACY RIGHTS may be RESTRICTED for the purposes of preventing or combating cybercrime during the DETECTION and INVESTIGATION of cybercrime.	
	Please describe whether, and if so, how, law that PROTECTS PRIVACY applies to computer data or electronic communication OUTSIDE of your country.	
	Please specify how law that PROTECTS PRIVACY applies to INVESTIGATIONS undertaken in YOUR COUNTRY by law enforcement AUTHORITIES from ANOTHER COUNTRY, in particular where informal cooperation is used.	

	Data Protection		If NO or IN PART
22	Please describe how law PROTECTS the handling of PERSONAL DATA. Please specify relevant legislation references and/or rulings.		
23	Does DATA PROTECTION LAW apply EQUALLY to ALL FORMS of data?		Please specify the BASIS on which DISTINCTIONS are made and the EFFECT of such distinctions
24	Please specify whether, and under what circumstances, EXCEPTIONS to DATA PROTECTION LAWS may be made for the purposes of preventing or combating cybercrime.		

Substantive and procedural criminal laws establish offences, investigatory measures, and punishments necessary for the prevention and combating of cybercrime. This legislation section contains questions about cyber-specific and general legislation governing cybercrime acts as well as procedural issues and cybercrime investigative measures.

Legislation governing criminal offences

		If YES				If NOT a criminal offence
		Are these acts covered by a CYBER-SPECIFIC or GENERAL CRIMINAL OFFENCE in your national law?	IF CYBER-SPECIFIC, please describe any MAIN DIFFERENCES between the definition in your law and the DESCRIPTION PROVIDED in this questionnaire	Please specify the LEGAL REFERENCE (Legislation name and article number or ruling) for the CYBER-SPECIFC and/or GENERAL offence	Please specify the minimum and maximum PENALTY for the offence	Please specify HOW these acts are addressed in law in your country
	Acts against (the confidentiality, integrity and availability of) computer data and systems					
25	Illegal access to a computer system				MIN:	
					MAX:	
26	Illegal access, interception or acquisition of computer data				MIN:	
					MAX:	
27	Illegal data interference or system damage				MIN:	
					MAX:	
28	Production, distribution or possession of computer misuse tools				MIN:	
					MAX:	
29	Breach of privacy or data protection measures				MIN:	
					MAX:	
	Computer-related acts for personal or financial gain					
30	Computer-related fraud or forgery				MIN:	
					MAX:	
31	Computer-related identity offences				MIN:	
					MAX:	
32	Computer-related copyright and trademark offences				MIN:	
					MAX:	
33	Sending or controlling sending of SPAM				MIN:	
					MAX:	
	Specific computer-related acts					
34	Computer-related acts causing personal harm				MIN:	
					MAX:	
35	Computer-related acts involving racism and xenophobia				MIN:	
					MAX:	
36	Computer-related production, distribution or possession of child pornography				MIN:	
					MAX:	
37	Computer-related solicitation or 'grooming' of				MIN:	

	children				MAX:		
38	Computer-related acts in support of terrorism offences				MIN:		
					MAX:		
39	Other (Please specify)				MIN:		
					MAX:		

			Please describe any EXCEPTIONS to the general rule
40	For the CRIMINAL OFFENCES listed above, please specify whether, IN GENERAL:	OFFENCES are limited to INTENTIONAL ACTS only?	
		ATTEMPTS to commit the offence are CRIMINALIZED?	
		ACTS PREPARATORY to the offence are CRIMINALIZED?	
		COMPANIES (or their DIRECTORS) can be CRIMINALLY LIABLE for the offence?	
		OMISSIONS are CRIMINALIZED?	

41	Does NATIONAL CRIMINAL LAW currently provide a SUFFICIENT framework for CRIMINALIZATION of acts of cybercrime ?		If YES
			Please describe the particular STRENGTHS and GOOD PRACTICE of your CRIMINAL law
			If NO or IN PART
			Please describe the MAIN GAPS in your CRIMINAL law

Legislation governing procedures and investigative measures

		Is the INVESTIGATIVE MEASURE authorized by CYBER-SPECIFIC law?	If yes, please specify the relevant LEGISLATION and ARTICLE number(s) or ruling	Is the INVESTIGATIVE MEASURE authorized by GENERAL CRIMINAL PROCEDURE law?	If yes, please specify the relevant LEGISLATION and ARTICLE number(s) or ruling
42	Search for computer hardware or data				
43	Seizure of computer hardware or data				
44	Order for subscriber information				
45	Order for stored traffic data				
46	Order for stored content data				
47	Real-time collection of traffic data				
48	Real-time collection of content data				
49	Expedited preservation of computer data				
50	Use of remote forensic tools				
51	Trans-border access to a computer system or data				
52	Other (Please specify)				

53	Does PROCEDURAL law currently provides a SUFFICIENT framework for INVESTIGATION of acts of cybercrime ?		If YES Please describe the particular STRENGTHS and GOOD PRACTICE of your PROCEDURAL law If NO or IN PART Please describe the MAIN GAPS in your PROCEDURAL law

Name of Respondent (Police):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

This section contains questions about the extent of cybercrime acts and offences encountered by and reported to police officials as well as threats, trends, and characteristics of cybercrimes encountered by police.

Police recorded offences and persons

		Are police STATISTICS for these acts available?	How many OFFENCES were recorded at the national level for the following years:			How many PERSONS were brought into formal contact for these acts for the following years:			Do statistics correspond to a CYBER-SPECIFIC offence or a GENERAL offence?	If CYBER-SPECIFIC, please describe any MAIN DIFFERENCES between the definition used for police statistics and the DESCRIPTION PROVIDED in this questionnaire
			2008	2009	2010	2008	2009	2010		
54	**Acts against (the confidentiality, integrity and availability of) computer data and systems**									
55	Illegal access to a computer system									
56	Illegal access, interception or acquisition of computer data									
57	Illegal data interference or system interference									
58	Production, distribution or possession of computer misuse tools									
59	Breach of privacy or data protection measures									
60	**Computer-related acts for personal or financial gain**									
61	Computer-related fraud or forgery									
62	Computer-related identity offences									
63	Computer-related copyright and trademark offences									
64	Sending or controlling sending of SPAM									

	Specific computer-related acts									
66	Computer-related acts causing personal harm									
67	Computer-related acts involving racism and xenophobia									
68	Computer-related production, distribution or possession of child pornography									
69	Computer-related solicitation or 'grooming' of children									
70	Computer-related acts in support of terrorism offences									
71	Other (please specify)									

72	If your country consists of a FEDERATION of STATES, do police statistics reported above cover BOTH federal and state levels?		If NO	Please specify which level is reported above	
73	Is a PRINCIPAL OFFENCE RULE used for counting offences reported above?				
74	How are MULTIPLE (serial) offences counted by police?				
75	Where statistics for an act above are NOT AVAILABLE, please describe why.				
76	Overall, is the current system of police statistics SUFFICIENT for RECORDING cybercrime acts?		If NO	Please specify what improvements are required	
77	How are police statistics used for POLICY DEVELOPMENT in combating cybercrime?				

Assessment of cybercrime trends and threats

78	HOW do cybercrime acts MOST FREQUENTLY come to the ATTENTION of the police?			
79	What MEASURES have been taken to INCREASE reporting of cybercrime to the police?			
80	On the basis of cybercrime acts encountered by police, what are the THREE MOST COMMON cybercrime acts in your country?			
81	What do you consider to be the THREE MOST significant cybercrime THREATS in your country (in terms of seriousness and loss or damage)?			
82	What PERCENTAGE of cybercrime acts are estimated to come to the ATTENTION of the police?		Please provide further comments	
83	On the basis of cybercrime acts encountered by police, what PERCENTAGE of acts involve a TRANSNATIONAL DIMENSION?		Please provide further comments	
84	What TRENDS in cybercrime acts have been observed in your country over the past FIVE years?			
85	What CHARACTERISTICS of cybercrime acts have been observed in your country over the past FIVE years?			
86	Please provide a short narrative describing a TYPICAL (real) cybercrime act RECENTLY IDENTIFIED by the POLICE.			

This section contains questions about procedural and investigatory measures concerning cybercrime and electronic evidence, as well as law enforcement cooperation in transnational cybercrime cases, organizational capacity and training.

Use of investigative measures

		Is this measure used by the police for INVESTIGATION of:		Who is legally entitled to AUTHORIZE this measure?	What are the legal REQUIREMENTS for using this measure?	What are the most common LEGAL and PRACTICAL obstacles to use of this measure?
		Cybercrime?	Non-cybercrime involving electronic evidence?			
87	Search for computer hardware or data					
88	Seizure of computer hardware or data					
89	Order for subscriber information					
90	Order for stored traffic data					
91	Order for stored content data					
92	Real-time collection of traffic data					
93	Real-time collection of content data					
94	Expedited preservation of computer data					
95	Use of remote forensic tools					

	Use of remote forensic tools					
96	Trans-border access to a computer system or data					
97	Other (Please specify)					

98	What are the THREE MOST COMMONLY USED measures for investigating cybercime?		
99	Please provide a short narrative describing GOOD PRACTICE for the use of a COMMON INVESTIGATIVE MEASURE in a TYPICAL (real) cybercrime case		
100	Do LIMITS and SAFEGUARDS on the use of investigative measures EXIST?		If YES Please DESCRIBE the limits and safeguards that are applied Please specify the legal basis of the limits and safeguards

Obtaining information from third parties and service providers

101	In general, can law enforcement agencies COMPEL persons or companies in your country who are NOT the DIRECT TARGET of an investigation to provide information?		If YES Please describe in WHAT WAYS

		Where such data is STORED	In REAL-TIME
102	Subscriber		

Please describe the PRACTICAL and LEGAL procedures (such as a police letter or court order) used to obtain the following information from service providers:	Subscriber information		
	Traffic data		
	Content data		

			If YES
			Please specify the NATURE of the relationship and the TYPE of INFORMATION exchanged on an INFORMAL BASIS
103	Do law enforcement agencies in your country maintain INFORMAL WORKING RELATIONSHIPS with service providers?		
104	Please provide a short narrative describing GOOD PRACTICE for obtaining information relevant to a cybercrime investigation from a SERVICE PROVIDER.		

Cooperation in cross-national investigations

105	How do law enforcement agencies in your country MOST OFTEN OBTAIN the following types of electronic evidence LOCATED in ANOTHER JURISDICTION:	Data stored on a suspect's computer?	
		Subscriber information from a service provider?	
		Traffic data from a service provider?	
		Content data from a service provider?	
106	If INFORMAL COOPERATION with law enforcement agencies in other countries is used in cybercrime investigations, please specify:	The EXTENT to which informal cooperation is used rather than formal/MLA channels	
		WHO is authorized to decide which method of cooperation should be	

	method of cooperation should be used	
	With WHICH COUNTRIES forms of informal cooperation in the area of cybercrime have been established	
	The FORMS of informal cooperation available from law enforcement agencies in your country (without need for a formal/MLA request)	

107 If your country has designated a FOCAL POINT for cooperation in cybercrime (such as a 24/7 NETWORK POINT OF CONTACT), please specify:

Which INSTITUTION serves as the FOCAL POINT								
The THREE MOST COMMON cybercrime acts to which requests relate								
The THREE MOST COMMON TYPES of requests								
The AVERAGE TIME taken (IN DAYS) for a RESPONSE		REQUESTS SENT				REQUESTS RECEIVED		
The number of REQUESTS RECEIVED AND SENT by the focal point in the following years		REQUESTS SENT				REQUESTS RECEIVED		
		2008	2009	2010		2008	2009	2010

108 Is TRANS-BORDER access to a computer system or computer data in your country by FOREIGN law enforcement agencies permissible:

		If YES
		Please specify under WHICH AGREEMENTS
Where bilateral or multilateral cooperation agreements exist?		
		Please specify under WHAT CIRCUMSTANCES
In the absence of bilateral or		

	In the absence of bilateral or multilateral cooperation agreements?		

Capacities and electronic evidence

			If YES: Please briefly describe AVAILABLE RESOURCES
109	Do law enforcement agencies in your country have SUFFICIENT RESOURCES (electricity, hardware, software, internet access) to use such INVESTIGATIVE MEASURES and to analyse ELECTRONIC EVIDENCE?		

			If YES: Please briefly describe AVAILABLE CAPACITIES
110	Do law enforcement agencies in your country have the CAPABILITY to carry out electronic forensics, including through forensic examination software?		

111	Please describe how ELECTRONIC EVIDENCE is:	Collected in a way that maintains the integrity of the evidence	
		Stored to protect against degradation or damage	
		Transferred to the prosecutor or court for use in a criminal trial	

			If YES: How do law enforcement agencies ADDRESS this challenge?
112	Is ELECTRONIC EVIDENCE often ENCRYPTED by suspects?		

Institutional capacity and training

113	Which description best matches the LAW ENFORCEMENT STRUCTURE for preventing and combating cybercrime in your country?	
114	If NO SEPARATE agency or unit exists for the investigation of cybercrime, are there PLANS to CREATE any new such	

	cybercrime, are there PLANS to CREATE any new such structure?			
115	How many SPECIALIZED OFFICERS are assigned to investigating cybercrime?	FULL TIME		PART TIME
116	How would you rate the TECHNICAL CAPACITIES of SPECIALIZED OFFICERS?			
117	What SUBJECT MATTER AREAS are covered by training received by SPECIALIZED OFFICERS?			
118	How often do SPECIALIZED OFFICERS receive TRAINING on the investigation of cybercrime?			
119	WHO is responsible for providing TRAINING to SPECIALIZED OFFICERS?			
120	Do regular (NON-SPECIALIZED) OFFICERS receive TRAINING in the investigation of cybercrime?			

Name of Respondent (Prosecution):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

This section contains questions about cybercrime acts and caseload volume for persons prosecuted for cybercrime as well as cybercrime trends and threats as perceived by prosecutors.

Prosecution cases and persons prosecuted

		Are prosecution STATISTICS corresponding to these acts available?	IF YES					Please describe any special CHARACTERISTICS of these acts noted by prosecutors
			Do statistics correspond to a CYBER-SPECIFIC offence or a GENERAL offence?	If CYBER-SPECIFIC, please describe any MAIN DIFFERENCES between the definition used for PROSECUTION statistics and the DESCRIPTION PROVIDED in this questionnaire	How many PERSONS were prosecuted at the NATIONAL level for the following years:			
					2008	2009	2010	
121	Acts against (the confidentiality, integrity and availability of) computer data and systems							
122	Illegal access to a computer system							
123	Illegal access, interception or acquisition of computer data							
124	Illegal data interference or system interference							
125	Production, distribution or possession of computer misuse tools							
126	Breach of privacy or data protection measures							
127	Computer-related acts for personal or financial gain							
128	Computer-related fraud or forgery							
129	Computer-related identity offences							
130	Computer-related copyright and trademark offences							
131	Sending or controlling sending of SPAM							

132	**Specific computer-related acts**							
133	**Computer-related acts causing personal harm**							
134	**Computer-related acts involving racism and xenophobia**							
135	**Computer-related production, distribution or possession of child pornography**							
136	**Computer-related solicitation or 'grooming' of children**							
137	**Computer-related acts in support of terrorism offences**							
138	**Other (please specify)**							

Assessment of cybercrime trends and threats

139	**What do you consider to be the THREE MOST significant cybercrime THREATS in your country (in terms of seriousness and loss or damage)?**	
140	**What TRENDS in cybercrime acts have been observed in your country over the past FIVE years?**	

This section contains questions on good practices and challenges, electronic evidence, organizational structure, specialization, and training of prosecution agencies and personnel with respect to cybercrime.

Good practices and challenges

141	In general, what are the most common LEGAL and PRACTICAL OBSTACLES to the successful prosecution of cybercrime acts?	
142	Please provide a short narrative describing GOOD PROSECUTION PRACTICE in a TYPICAL (REAL) cybercrime case RECENTLY handled by prosecutors.	

Electronic evidence

			If YES
			Please specify the LEGISLATION and ARTICLE number(s) or RULING
143	Is a DISTINCTION made IN LAW between ELECTRONIC and (TRADITIONAL) PHYSICAL EVIDENCE?		
			Please provide the DEFINITION of 'ELECTRONIC EVIDENCE'
144	Is ELECTRONIC EVIDENCE ADMISSIBLE before a court in CRIMINAL PROCEEDINGS?		

			If YES
			Please specify in what way ADMISSIBILITY rules DIFFER
145	Do ADMISSIBILITY rules DIFFER for ELECTRONIC EVIDENCE obtained from OUTSIDE the JURISDICTION?		
146	Please describe any OTHER specific RULES that apply ONLY to ELECTRONIC EVIDENCE		

			If YES
			Please specify the LEGISLATION and ARTICLE number(s) or RULING
147	Has your country developed EVIDENTIARY LAWS specifically for CYBERCRIME?		
			Please SUMMARIZE the MAIN provisions
148	Please describe approaches taken by prosecutors to ESTABLISH a clear LINK between ELECTRONIC EVIDENCE and a SPECIFIC PERPETRATOR.		

			If YES
			Please briefly describe AVAILABLE RESOURCES
149	Do prosecution agencies in your country have SUFFICIENT RESOURCES (electricity, hardware, software, internet access) to HANDLE and to ANALYSE ELECTRONIC EVIDENCE?		
150	Please specify the TECHNICAL MEANS by which ELECTRONIC EVIDENCE is PRESENTED by prosecutors to the court in a CRIMINAL TRIAL.		

		What are the most common LEGAL and PRACTICAL obstacles to use of electronic evidence obtained by THIS INVESTIGATIVE MEASURE in SUCCESSFUL PROSECUTIONS?	Please identify what LEGISLATION, amendments or PRACTICAL MEASURES could be used to address these issues
151	Search for and seizure of computer hardware or data		
152	Order for stored subscriber information, traffic data or content data		
153	Real-time collection of traffic data or content data		
154	Use of remote forensic tools		

155	Trans-border access to a computer system or data		
156	Other (Please specify below)		

Institutional capacity and training

157	Which description best matches the PROSECUTION STRUCTURE for investigation and prosecution of cybercrime in your country?			
158	If NO SEPARATE agency or unit exists for the prosecution of cybercrime, are there PLANS to CREATE any new such structure?			
159	How many SPECIALIZED PROSECUTORS are assigned to investigating cybercrime?	FULL TIME		PART TIME
160	How would you rate the TECHNICAL CAPACITIES of SPECIALIZED PROSECUTORS?			
161	What SUBJECT MATTER AREAS are covered by training received by SPECIALIZED PROSECUTORS assigned to the investigation and prosecution of cybercrime?			
162	How often do SPECIALIZED PROSECUTORS receive TRAINING on the investigation of cybercrime?			
163	WHO is responsible for providing TRAINING to SPECIALIZED PROSECUTORS?			
164	Do regular (NON-SPECIALIZED) prosecutors receive TRAINING in the investigation of cybercrime?			

Name of Respondent (Court):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

This section contains questions about cybercrime acts and caseload volume for persons brought before the court as well as questions on organizational structure, specialization, and training of courts and personnel with respect to cybercrime.

Court cases and persons convicted

		Are court STATISTICS corresponding to these acts available?	IF YES					Please describe any special CHARACTERISTICS of these acts noted by the courts
			Do statistics correspond to a CYBER-SPECIFIC offence or a GENERAL offence?	If CYBER-SPECIFIC, please describe any MAIN DIFFERENCES between the definition used for COURT statistics and the DESCRIPTION PROVIDED in this questionnaire	How many PERSONS were convicted at the national level for the following years:			
					2008	2009	2010	
165	**Acts against (the confidentiality, integrity and availability of) computer data and systems**							
166	Illegal access to a computer system							
167	Illegal access, interception or acquisition of computer data							
168	Illegal data interference or system interference							
169	Production, distribution or possession of computer misuse tools							
170	Breach of privacy or data protection measures							
171	**Computer-related acts for personal or financial gain**							
172	Computer-related fraud or forgery							
173	Computer-related identity offences							
174	Computer-related copyright and trademark offences							
175	Sending or controlling sending of SPAM							

176	**Specific computer-related acts**							
177	**Computer-related acts causing personal harm**							
178	**Computer-related acts involving racism and xenophobia**							
179	**Computer-related production, distribution or possession of child pornography**							
180	**Computer-related solicitation or 'grooming' of children**							
181	**Computer-related acts in support of terrorism offences**							
182	**Other (Please specify)**							

Good practices and challenges

183	**From the perspective of the COURT, please describe the important ELEMENTS for a SUCCESSFUL CONVICTION in cybercrime cases.**	
184	**In general, what are the most common LEGAL and PRACTICAL obstacles to the successful convictions in cybercrime cases?**	
185	**Please provide a short narrative describing GOOD COURT PRACTICE in a TYPICAL (REAL) cybercrime case RECENTLY handled by the courts.**	**Where available, please attach a SUMMARY or FULL JUDGMENT OF THE CASE described above, or provide a direct WEB LINK to publicly available judgments**

Institutional capacity and training

186	**Which description best matches the COURT STRUCTURE for CYBERCRIME CRIMINAL cases in your country?**	

187	If NO SEPARATE court structure exists for CYBERCRIME CRIMINAL cases, are there PLANS to CREATE any new such structure?			
188	How many SPECIALIZED JUDGES are assigned to investigating cybercrime?	FULL TIME		PART TIME
189	What SUBJECT MATTER AREAS are covered by training received by SPECIALIZED JUDGES assigned to CYBERCRIME CRIMINAL cases?			
190	How often do SPECIALIZED JUDGES receive TRAINING on the investigation of cybercrime?			
191	WHO is responsible for providing TRAINING to SPECIALIZED JUDGES?			
192	Do regular (NON-SPECIALIZED) JUDGES receive TRAINING in the investigation of cybercrime?			

Name of Respondent (Extradition):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

Various forms of international cooperation are essential to the prevention and combating of cybercrimes which are often transnational in character. This section contains questions on authority, mechanisms, requests sent and received, volumes, and outcomes with respect to extradition for cybercrime offences.

Extradition authority and request processing

			If YES
193	Does your country have LEGISLATION used as a legal basis for sending and receiving EXTRADITION REQUESTS on cybercrime?		Please provide the name of relevant legislation OR provide a direct WEB LINK to the full text of the instrument

			If NO or under CERTAIN CONDITIONS
			Please provide further details
194	In general, are CYBERCRIME ACTS EXTRADITABLE offences?		
195	Please identify the CENTRAL AUTHORITY responsible for receiving and sending EXTRADITION requests In CRIMINAL INVESTIGATIONS or CASES involving cybercrime.		
196	Which AUTHORITY is RESPONSIBLE for DECISIONS on EXTRADITION requests RECEIVED in your country?		
197	What forms of COMMUNICATION in cybercrime EXTRADITION cases are usually used?		

198	What are the PRE-CONDITIONS that must be met before an EXTRADITION request in cybercrime cases can be CONSIDERED?				
199	Can PROVISIONAL ARREST be ordered with respect to EXTRADITION requests in cybercrime cases?		If YES	Please provide details of the conditions required	
200	Please specify any MULTILATERAL COOPERATION groups of which your country is a member for the purposes of EXTRADITION.				

Mechanisms for extradition requests

		Please specify the NUMBER of CYBERCRIME EXTRADITION REQUESTS that used the following mechanisms for the MOST RECENT YEAR where statistics are available		Please provide comments on CHALLENGES encountered and GOOD PRACTICES used with respect to the INSTRUMENT
201	Please specify the YEAR to which statistics refer:			
		SENT	RECEIVED	
202	Multilateral instruments (Please specify)			
203	Regional treaties (Please specify)			
204	Bilateral treaties (Please specify)			
205	Reciprocity in the absence of treaty provision			
206	Other (Please specify)			
207	TOTAL			

Extradition requests received and granted

		How many EXTRADITION REQUESTS were RECEIVED for the following years:			How many EXTRADITION REQUESTS were SENT for the following years:			From which COUNTRIES were extradition REQUESTS most frequently RECEIVED?	To which COUNTRIES were extradition REQUESTS most frequently SENT?
		2008	2009	2010	2008	2009	2010		
208	Acts against (the confidentiality, integrity and availability of) computer data and systems								
209	Computer-related acts for personal or financial gain								
210	Specific computer-related acts								
211	Other (Please specify)								

212	For EXTRADITION REQUESTS described in the table above, are REQUESTS SENT and RECEIVED counted SEPARATELY where MULTIPLE ACTS are included within a SINGLE REQUEST?		If NO	Please describe the basis on which they are counted:

		REQUESTS RECEIVED	REQUESTS SENT
213	For cybercrime EXTRADITION REQUESTS SENT AND RECEIVED, please estimate the AVERAGE TIME for a response.		
		Please provide any additional relevant information about the time taken to receive a response.	

214	What is the MOST COMMON REASON for an EXTRADITION REQUEST in a cybercrime case to be rejected by your country?	
215	Please provide a short narrative describing GOOD EXTRADITION PRACTICE(S) a recent TYPICAL (real) cybercrime case.	

Name of Respondent (Mutual Legal Assistance):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

Various forms of international cooperation are essential to the prevention and combating of cybercrimes which are often transnational in character. This section contains questions on authority, mechanisms, volume, requests sent and received, and outcomes with respect to mutual legal assistance (MLA) in cybercrime investigation and control activities.

Mutual legal assistance authority and request processing

			If YES
216	Does your country have LEGISLATION used as a legal basis for MUTUAL LEGAL ASSISTANCE (MLA) for cybercrime?		Please provide the name of relevant legislation OR provide a direct WEB LINK to the full text of the instrument
217	Please identify the CENTRAL AUTHORITY responsible for receiving and sending requests for MLA in CRIMINAL INVESTIGATIONS or CASES involving cybercrime.		
218	Which AUTHORITY is RESPONSIBLE for DECISIONS on MUTUAL LEGAL ASSISTANCE requests RECEIVED in your country?		
219	What forms of COMMUNICATION in cybercrime MLA cases are usually used?		
220	What are the PRE-CONDITIONS that must be met before an MLA request in cybercrime cases can be CONSIDERED?		

221	What MLA ACTIONS may be requested from your country in cybercrime cases?		
222	Do specific channels exist for URGENT requests for MLA in cybercrime cases?		
223	Can assistance be provided by your country through INFORMAL COOPERATION (such as direct POLICE cooperation) as well as through a formal MLA request?		If YES: Please describe the relationship between informal cooperation channels and MLA requests
224	Does your country have a POLICY or REGULATIONS for the type of assistance that can be provided through INFORMAL COOPERATION and the type that must be provided through MLA?		If YES: Please describe the MAIN ELEMENTS of the POLICY or REGULATIONS
225	Please specify any MULTILATERAL COOPERATION groups of which your country is a member for the purposes of MLA		

Mechanisms for MLA requests

		Please specify the NUMBER of CYBERCRIME MLA REQUESTS that used the following mechanisms for the MOST RECENT YEAR where statistics are available		Please provide comments on CHALLENGES encountered and GOOD PRACTICES used with respect to the INSTRUMENT
226	Please specify the YEAR to which statistics refer:			
		SENT	RECEIVED	
227	Multilateral instruments (Please specify)			
228	Regional treaties (Please specify)			

229	Bilateral treaties (Please specify)			
230	Reciprocity in the absence of treaty provision			
231	Other (Please specify)			
232	TOTAL			

MLA requests received and sent

		How many MLA REQUESTS were RECEIVED for the following years:			How many MLA REQUESTS were SENT for the following years:			From which COUNTRIES were MLA REQUESTS most frequently RECEIVED?	To which COUNTRIES were MLA REQUESTS most frequently SENT?
		2008	2009	2010	2008	2009	2010		
233	Acts against (the confidentiality, integrity and availability of) computer data and systems								
234	Computer-related acts for personal or financial gain								
235	Specific computer-related acts								
236	Other (Please specify)								

237	For MLA REQUESTS described in the tables above, are REQUESTS SENT and RECEIVED counted SEPARATELY where MULTIPLE ACTS are included within a SINGLE REQUEST?		If NO	Please describe the basis on which they are counted:	

		REQUESTS RECEIVED		REQUESTS SENT
238	For cybercrime MLA REQUESTS SENT AND RECEIVED, please estimate the AVERAGE TIME for a response.			
		Please provide any additional relevant information about the time taken to receive a response.		
239	What is the MOST COMMON REASON for an MLA REQUEST in a cybercrime case to be rejected by your country?			
240	Please provide a short narrative describing GOOD MLA PRACTICE(S) from a recent TYPICAL (real) cybercrime case.			

Name of Respondent (Technical Assistance):	
Functional Title:	
Agency:	
Street:	
City/State/Country:	
Email Address:	
Telephone (country code, area code, number):	
Fax (country code, area code, number):	

Various forms of international cooperation are essential to the prevention and combating of cybercrimes which are often transnational in character. This section contains questions on authority, mechanisms, requests sent and received, volumes, and outcomes with respect to technical assistance in cybercrime investigation and control activities.

Technical assistance received

241	Has your country RECEIVED TECHNICAL ASSISTANCE from an international organization, another country, or the private sector related to the prevention and combating of cybercrime?	

		If YES		
		Programme/project 1	Programme/project 2	Programme/project 3
242	Please identify up to THREE major technical assistance programmes or projects from which your country has benefited in the last three years			
243	Please specify the THEMATIC AREA(S) in which technical assistance was received			
244	Please specify which INSTITUTION(S) received technical assistance.			
245	Please specify which ORGANIZATION or DONOR supported the technical assistance			
246	Please specify the DURATION of technical assistance			
247	Please specify who DELIVERED the technical assistance			
248	Please specify the total VALUE of technical assistance delivered by the programme/project			

249	Please specify EVALUATION OUTCOMES of technical assistance received			

250	Does your country REQUIRE technical assistance related to the prevention and combating of cybercrime?	

		If YES		
		Thematic area 1	Thematic area 2	Thematic area 3
251	Please specify up to three THEMATIC AREA(S) in which technical assistance is required			
252	Please specify which INSTITUTION(S) would require assistance in this thematic area			

Technical assistance delivered

253	Has your country DELIVERED technical assistance to another country related to the prevention and combating of cybercrime?	

		If YES		
		Programme/project 1	Programme/project 2	Programme/project 3
254	Please identify up to THREE major technical assistance programmes or projects which your country has provided in the last three years			
255	Please specify the THEMATIC AREA(S) in which technical assistance was provided			
256	Please specify to which INSTITUTION(S) technical assistance was provided. Please provide details of the full name of the institution and unit within the institution			

257	Please specify which country or countries RECEIVED the technical assistance			
258	Please specify the DURATION of technical assistance			
259	Please specify who DELIVERED the technical assistance			
260	Please specify the total VALUE (in USD) of technical assistance DELIVERED by the programme/project			
261	Please describe EVALUATION OUTCOMES of technical assistance delivered			