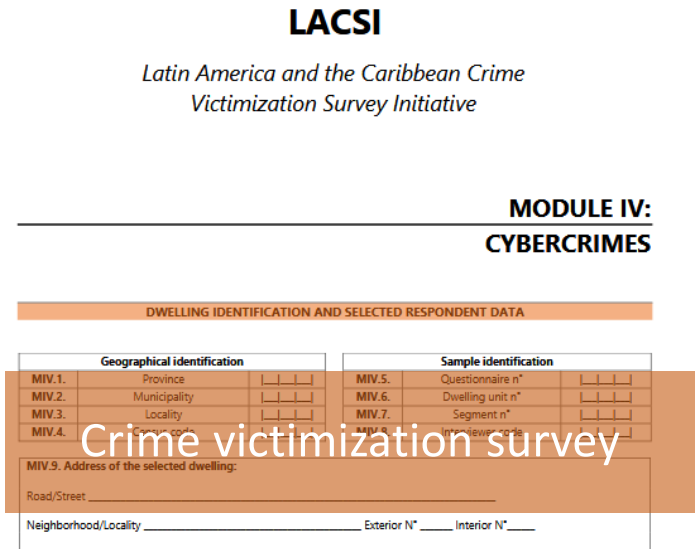
International efforts to harmonize the measurement of cybercrime

World Telecommunication/ICT Indicators Symposium (WTIS)

David Rausis, Research and Trend Analysis Branch, UN Office on Drugs and Crime

Measuring cybercrime – International harmonization

Administrative data from criminal justice system



Crime victimization survey

	Convention Article	ICCS Code	CY tag	ICCS offense	ICCS offense desc
	Article 7	09031	X	Unlawful access to a computer system	Unlawful acts involving entry into parts or t without authorization or justification
	Article 8	09033	X	Unlawful interception or access of computer data	Unlawful acts involving gaining access to c authorization or justification, including obta transmission process that is not intended t computer data (such as by copying data) w
a	Article 9	090322	X	Unlawful interference with computer data	Acts involving damage, deletion, deteriorati suppression of computer data without auth justification.
and stem	Article 10	090321	X	Unlawful interference with a computer system	Unlawful acts hindering the functioning of a system.
	Article 11	09039	X	Other acts against computer systems	Acts against computer systems not describ categories 09031 – 09033
ns ery	Article 12	0702	(Cy)	Forgery/counterfeiting	Creating, manufacturing, selling, passing or goods, or an instrument to create a false im
ns t or fraud	Article 13	0701	(Cy)	Fraud	Obtaining money or other benefit or evadin dishonest conduct.
sexual on	Article 14	030221	(Cy)	Child pornography	Procuring, arranging, facilitating or controll purposes of creating child pornography and disseminating, broadcasting, transmitting, selling child pornography
purpos against a	Article 15	030223	(Cy)	Sexual grooming of children	Sexual grooming of a child with a chi Internet and exposing them to sexually exp with a child in person to expose them gradu
of	Article 16	0719	(Cy)	Other acts against exploitation	Sexual exploitation of children, not classif 030223 - Sexual exploitation as de in 0
e	Article 17	0704	(Cy)	Acts involving the proceeds of crime	Receiving, handling or processing money or obtained, directly or indirectly, through the

Draft statistical framework for measuring cybercrime (ongoing)

Administrative data on cybercrime from the criminal justice system

Benefits

→ Part of the regular crime statistics for some offences.

→ Improve understanding of cybercrime and its impact on the population.

→ Build cases for legislative changes for investigation and penalization.

Factors affecting comparability and interpretation

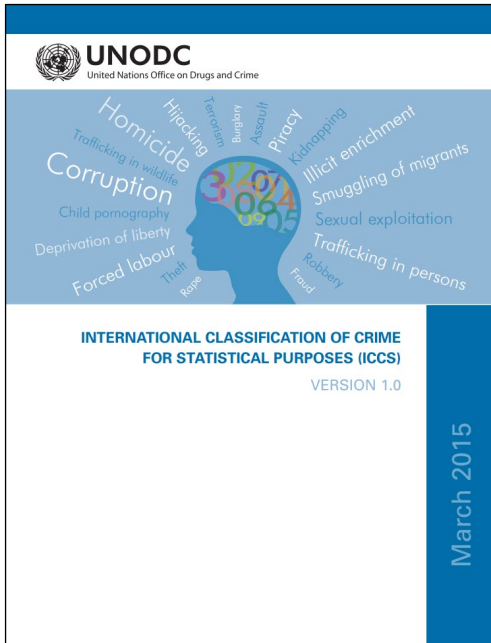
→ The number of crimes which are reported/detected

→ The way in which crime is registered and counted

→ **The way in which crime is defined and classified**

International Classification of Crime for Statistical Purposes (ICCS)

- Approved in 2015 by UN Statistical Commission and UN Commission on Crime Prevention and Criminal Justice
- International statistical standard for crime data collection
- Based on the description of behaviours and acts, not on criminal laws, which means it is equivalent for all jurisdictions.
- Available in all 6 UN languages



Cybercrime in the International Classification of Crime for Statistical Purposes

Cyber-dependent crime

0903			Acts against computer systems
	09031		Unlawful access to a computer system
	09032		Unlawful interference with a computer system or computer data
		090321	Unlawful interference with a computer system
		090322	Unlawful interference with computer data
	09033		Unlawful interception or access of computer data
	09039		Other acts against computer systems

09031 Unlawful access to a computer system

Unlawful acts involving entry into parts or the whole of a computer system without authorization or justification.[129]
- Computer systems as defined in footnote 128.

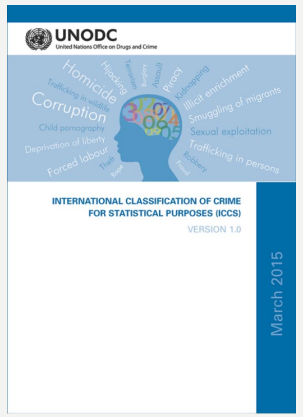
\+ **Inclusions:** Access to a computer system without right; hacking

\- **Exclusions:** Unlawful access to private computer files that amounts to intrusions upon one's privacy (02011); apply all exclusions listed in 0903

- Offences that target a computer or a computer system per se.
- Can only be committed through an ICT infrastructure
- Examples:
  - Hacking, denial of service attacks, dissemination of malware, …
- Should be classified under specific categories (e.g., unlawful access to a computer system).

Cybercrime in the International Classification of Crime for Statistical Purposes

Cyber-enabled crime



ICCS

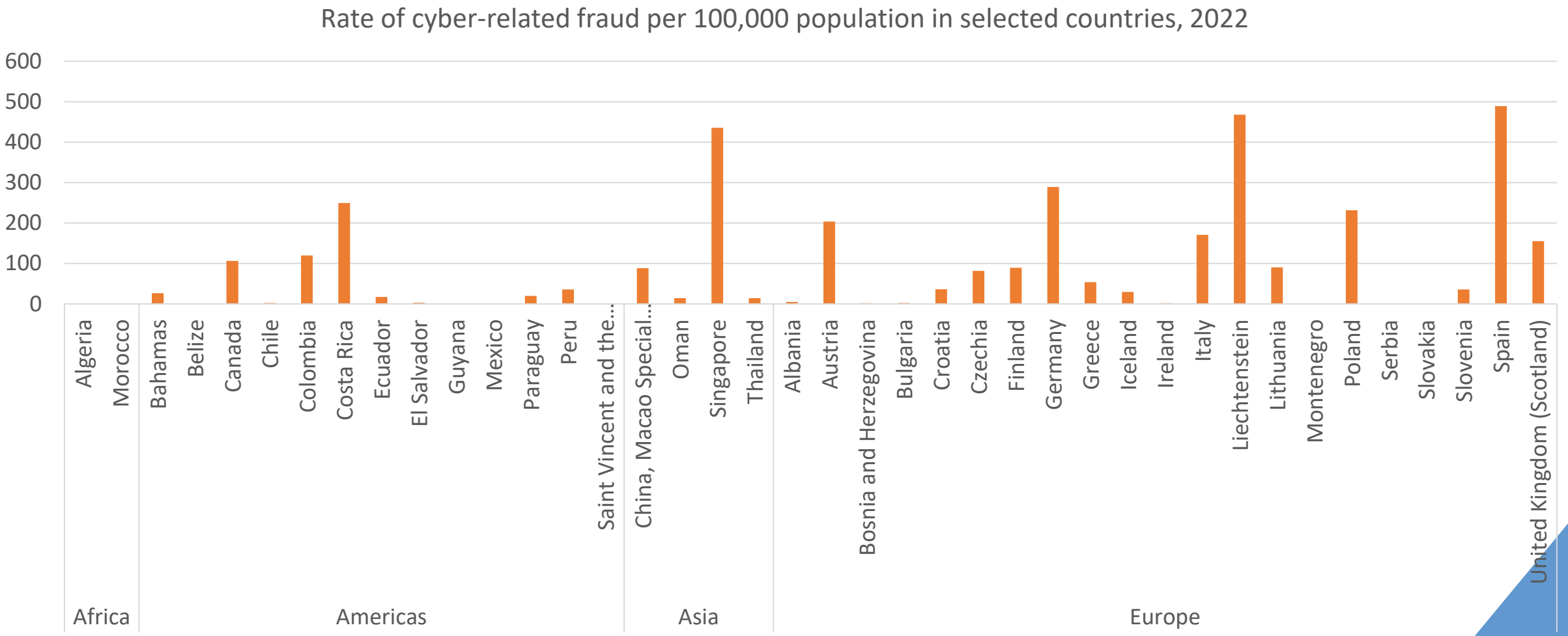
EVENT DISAGGREGATIONS
At – Attempted/Completed
We – Type of weapon used
SiC – Situational context
Geo – Geographic location
DaT – Date and time
Lo – Type of location
Mot – Motive
Cy – Cybercrime related
Rep – Reported by

Disaggregating variables

Cy - Cybercrime related

- Offences where computers are used to commit traditional crimes such as theft, harassment or fraud.
- To be classified under respective crime with a tag to identify if the crime was committed with the use of a computer (e.g., harassment with a tag to show it was committed through text messages or social media).

Example of global data on cybercrime



Crime victimization survey

- To collect information on the perception of security and victimization experience.
- Criminal acts are described instead of using criminal code.
- Provides information on hidden figure of crime and experience in reporting the crime.
- Includes information on characteristics of the victim, the offender and the event.
- Measure economic and social consequences of the crime.

United Nations
Office on Drugs and Crime

UNODC-INEGI CENTER OF EXCELLENCE
in Statistical Information on Government,
Crime, Victimization and Justice

Latin America and the Caribbean Crime Victimization Survey Initiative (LACSI)

Survey questionnaire available in English, Spanish, Portuguese and French at this page.

Victimization survey module: Cybercrimes

- Could you tell me what type of situation (cybercrime) did you suffer?
  1. Cyberbullying
  2. Email hacking
  3. Social media hacking
  4. Identity theft/impersonation
  5. Malware
  6. Ransomware

Social media hacking: Someone gained access to your online social account(s) without your permission such as Facebook, Twitter, Instagram, LinkedIn, blogs, etc. and resulted in any messages or posts being made from your social media account(s) that you did not send.

- Specific questions for each cybercrime
- Questions for all cybercrimes
  - Date, financial loss, effects on physical and mental health, other negative effects, reporting to authorities

Countries of Latin American and Caribbean that have collected data on cybercrime or digital security incidents based on the LACSI initiative

With data:

Bolivia 2023
Chile 2023
Colombia 2023
Dominican Republic 2022
Saint Lucia 2020

In data collection

-Uruguay, 2025

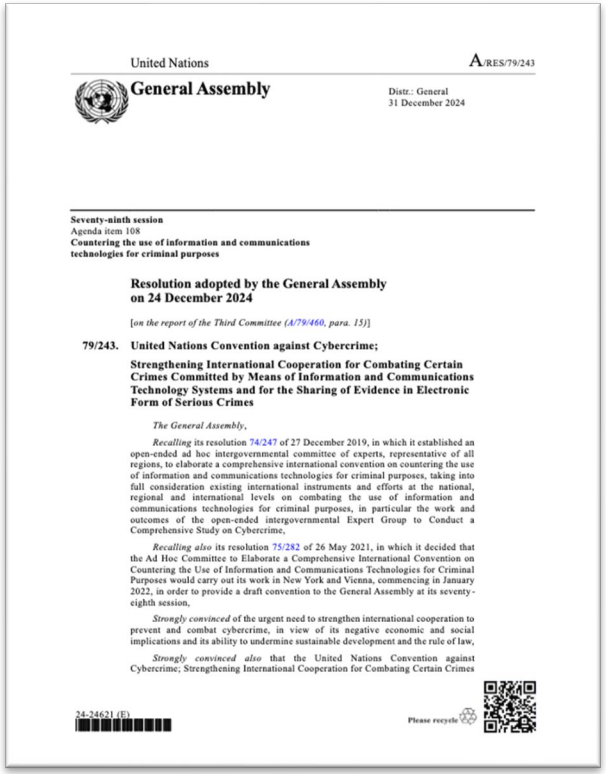
Countries that have their own measurements:

Peru, 2024
Mexico, 2024

Crime victimization survey: Challenges

Lack of legal definition of cyber-dependent, cyber-enabled or technology-facilitated offences.	• Reluctance to measure events that are not explicitly codified in national law.
"Hacking" can occur through channels beyond those typically listed (social media and e-mail) in the survey.	• Scope and classification issues linked to the limits of victimization surveys.
Module covers individuals aged 18 years and over.	• Offences that disproportionately affect children and adolescents (e.g., online grooming) are therefore likely to be under-represented.
Fraud and scams (including those perpetrated through electronic means) covered in another module.	• Not measured as part of cybercrime.
Lists of platforms/examples (devices) rapidly obsolete in the face of new environments (crypto-wallets, deepfakes, work/educational accounts).	• Need for regular updates.
Module captures reporting and satisfaction with competent authority and reasons for not reporting, but many cases are resolved with platforms or involve cross-border actors.	• Lack granularity for international cooperation and non-criminal avenues.

United Nations Convention against Cybercrime



United Nations A/RES/79/243

General Assembly Distr.: General
31 December 2024

Seventy-ninth session
Agenda item 108
Countering the use of information and communications technologies for criminal purposes

Resolution adopted by the General Assembly on 24 December 2024

[on the report of the Third Committee (A/79/460, para. 15)]

79/243. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

The General Assembly,

Recalling its resolution 74/247 of 27 December 2019, in which it established an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime,

Recalling also its resolution 75/282 of 26 May 2021, in which it decided that the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes would carry out its work in New York and Vienna, commencing in January 2022, in order to provide a draft convention to the General Assembly at its seventy-eighth session,

Strongly convinced of the urgent need to strengthen international cooperation to prevent and combat cybercrime, in view of its negative economic and social implications and its ability to undermine sustainable development and the rule of law,

Strongly convinced also that the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes

24-24621 (E)

Please recycle

United Nations Convention against Cybercrime;
Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

- 24 December 2024: Adoption of the UN Convention by the General Assembly (Resolution 79/243)
- 25-26 October 2025: Signing ceremony
- 2025 onward: Ratification by States and entry into force
- Held periodically: Conference of the States parties

UN Convention against Cybercrime - Criminalization

Article	Chapter II. Criminalization
7	Illegal access
8	Illegal interception
9	Interference with electronic data
10	Interference with an information and communications technology system
11	Misuse of devices
12	Information and communications technology system-related forgery
13	Information and communications technology system-related theft or fraud
14	Offences related to online child sexual abuse or child sexual exploitation material
15	Solicitation or grooming for the purpose of committing a sexual offence against a child
16	Non-consensual dissemination of intimate images
17	Laundering of proceeds of crime

Cyber-dependent crimes

Cyber-enabled crimes

Statistical Framework to Measure Cybercrime

Issues brought forward during first consultation

- Adaptation of existing crime classification.
- Definition of cybercrime for statistical purpose.
- Inclusion of privately held data.
- Inclusion of financial loss as an indicator.
- Inclusion of indicators related to cybercrime prevention policies.
- Addressing the intertwined nature of cybercrime types, such as personal data breaches leading to fraud and the spread of illegal digital content.

Possible indicators framework (based on corruption measurement framework)

<table>
<tr><td rowspan="4">Criminal offence</td><td colspan="2">Direct measures: Prevalence of cybercrime</td></tr>
<tr><td rowspan="3">Indirect measures</td><td>Perception: How much cybercrime is perceived</td></tr>
<tr><td>Risk: How high are the risks of cybercrime</td></tr>
<tr><td>Response: What is the scale of government response</td></tr>
</table>

Thank you very much for your attention!

- We welcome suggestions for the development of a draft cybercrime measurement framework.

- Contact: rausis@un.org