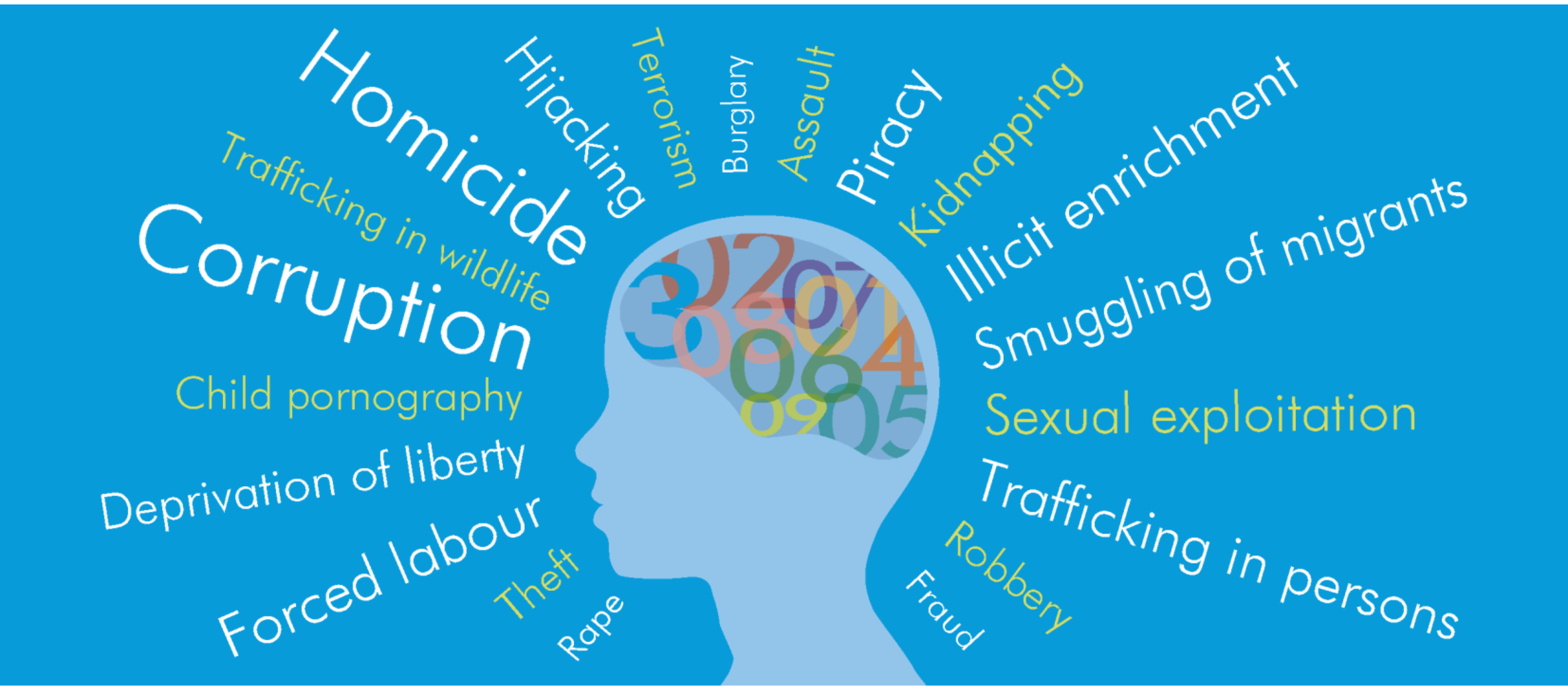
UNODC
United Nations Office on Drugs and Crime

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

UNODC Research

2 ICCS Advocacy Brief

Measuring cybercrime through the ICCS lens



July 2023

Measuring cybercrime through the ICCS lens

What is the International Classification of Crimes for Statistical Purposes (ICCS)?

The ICCS is a statistical classification, a set of discrete, exhaustive, and mutually exclusive categories which can be assigned to one or more variables used in the collection and presentation of data from criminal activities. It is a comprehensive framework of internationally agreed crime concepts and definitions which enhance the collection, organization, analysis, and dissemination of statistical data on crime, including the characteristics of criminal acts, victims, perpetrators, motives, and other essential data.

The ICCS is therefore a statistical tool to understand the extent and drivers of crime. Its primary unit of classification is the act or event that constitutes a criminal offence, and the description of the criminal act is based on mutually exclusive behaviors rather than legal provisions. Since 2015, it has helped to improve the coherence and international comparability of crime statistics and enhance the capacity for analysis, both nationally and internationally.[1]

Why is it relevant to measure cybercrime through the ICCS?

Society has dramatically changed since the adoption and evolution of Information and Communications Technology (ICT), which have revolutionized the way people connect. As society adopted ICTs, the range of crimes that could be committed using them became ever-changing, both in terms of technological change and in terms of social interaction with the new technologies. Since its conception, the ICCS has acknowledged the relevance of producing data on cybercrime, and the use of ICTs in criminal activities. However, this need has become more pressing as a result of the COVID-19 pandemic. During the pandemic, there was an increase in phishing, credit card fraud, pirated websites asking for fake donations and cyber-attacks – including those orchestrated by organized criminal groups.[2]

What are the benefits of measuring cybercrime and other ICT used for criminal purposes?

Through the implementation of the ICCS, statistics on crime become more relevant for a number of cybercrime and ICT relevant issues, such as:

- Legislation on cybercrime: with the adoption of the behavior-based approach of the ICCS, national statistics on a number of cybercrimes or crimes committed using ICTs can be produced in a standardized and comprehensive manner. These cybercrime statistics can then build the case for legislative changes for investigation and penalization.

[1] The ICCS was endorsed by the United Nations Statistical Commission, at its 46th session in March 2015, and the Commission on Crime Prevention and Criminal Justice (CCPCJ) at its 24th session in May 2015 as an international statistical standard for data collection. The two Commissions have also confirmed UNODC as the custodian of the ICCS. For more information, visit: https://www.unodc.org/unodc/en/data-and-analysis/statistics/iccs.html

[2] The impact of COVID-19 on organized crime, Research Brief (United Nations Office on Drugs and Crime, 2020).

- Protection of victims: by making cybercrimes visible through statistics, a cybersecurity culture and awareness system can be put in place for individuals, businesses and organizations to protect themselves.
- Justice for victims: by making cybercrimes visible, victims can also seek justice in a system that penalizes these crimes.
- Cybercrime statistics: these can be used to get a better understanding and more accurate description of cybercrime, make evidence-based decisions, and encourage investigative staff to get trained and qualified to deal with the cybercrimes affecting a population.
- Promoting collaboration between Member States through strategic alliances for data exchange, research, analysis, and investigation, considering the transnational nature of cybercrime and the interdependence of systems and digital devices connected to the Internet within countries and beyond.
- Understanding better which mechanisms should be established to monitor the effects of cybercrime, by adopting or improving data collection tools adapted to this reality.

How are cybercrime and other ICTs used for criminal purposes measured through the ICCS?

The analysis of cybercrime and other ICTs used for criminal purposes is a cross-cutting element within the framework of the ICCS. The use of ICTs is identified by the ICCS as a factor that can facilitate various types of criminal behaviors. The classification is designed to systematically record the cyber dimension of offences, which facilitates the measurement of *cyber-dependent crimes*[3] and *cyber-enabled crimes*[4]. While these terms are currently not explicitly included in the ICCS, the classification can be used to distinguish between the two forms of cybercrime.

The ICCS establishes definitions of some specific *cyber-dependent crimes* under level 2 category 'Acts against computer systems' (0903). This includes, among others, hacking, denial of service attacks, deleting computer system files without authorization, computer system damage, the creation, dissemination and deployment of malware or ransomware, and attacks on critical national infrastructure.

Cyber-enabled crimes, however, do not have dedicated ICCS codes, as they are traditional crimes that are committed using a computer. To help identify these offences as cybercrimes, the ICCS offers the cybercrime-related (Cy) variable. It should be applied when the use of computer data or computer systems was a key part of the modus operandi of the crime.

Note that the cybercrime-related variable should also be used for *cyber-dependent crimes*. However, since these offences have dedicated ICCS codes, they can be identified as cybercrimes without using the variable. *Cyber-enabled crimes*, on the other, cannot be recognized in statistics as

[3] Cyber-dependent crimes are offences that target a computer or a computer system per se. These crimes can only be committed through an ICT infrastructure and are often criminalized as unauthorized access to, interception of, interference with, or misuse of computer data or computer / information systems. See footnote 128 (page 85) in the ICCS for definitions on computer data, computer/ information system, and computer/information program.

[4] Cyber-enabled crimes are offences where computers are used to commit traditional crimes such as theft, harassment or fraud. These are offences that can be committed without a computer but can also be facilitated by ICTs.

cybercrimes without the cybercrime-related variable.

How does the cybercrime-related variable work?

Certain characteristics of criminal events or their modus operandi can be recorded through the application of the ICCS using one of the variables included under the event disaggregations. These variables should be used at the individual record level and serve to assign specific information to each recorded criminal event.

The cybercrime-related variable is considered under event disaggregations. The variable can be used in conjunction with other disaggregating variables included in the ICCS to create a more complete picture of the crime. This includes the sex and age of both the victim and perpetrator, details on the victim-perpetrator relationship and date and time of the crime, among others. [5]

As noted above, crimes can be tagged using the cybercrime-enabled variable if the use of computer data or systems is a key part of the modus operandi of the crime. This considers crimes that can be committed in the physical world but are facilitated in the virtual world and can include online fraud, online drug purchases, cyberbullying, cyberharassment, threats, copyright infringement, money laundering, identity theft or impersonation, blackmail, defamation, sextortion, pornography offenses (including revenge porn and grooming), production and distribution of child pornography, among others.

Using this approach, it is possible to record and count cyber-related criminal offences in a comprehensive manner. Apart from crimes against computer systems themselves, the use of ICTs to commit crimes is not always explicit. The cybercrime-related variable provides more comprehensive information to identify all crimes committed using a cyber or virtual facilitator.

The cybercrime-related variable should not be applied when the use of ICTs is not a key part of the modus operandi of the crime. For example, it is recommended to use the cybercrime-related variable for an act of harassment that was committed through text messages or a social media account. The use of ICTs is a key part of the crime and this will then be recorded as an act of cyberbullying. On the other hand, if a homicide was committed by a perpetrator who located the victim by using his/her cellphone signal, the cybercrime-related tag should not be used. Here, the use of ICTs is not a key part of the crime. It is an incidental aspect of the homicide which provides electronic evidence that can be used, for instance, to determine intent and distinguish between intentional and non-intentional homicide.

What is being done to further improve the measurement of cybercrime through the ICCS?

Member States are negotiating a new convention on countering the use of information and communications technologies for criminal purposes which is scheduled to be presented at the 78th Session of the United Nations General Assembly. This is done through the work of the *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.*[6]

Once negotiations of the convention are finalized, future discussions could be

[5] For more detail, see tables II-V of the ICCS.

[6] For more information, visit: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

undertaken between UNODC and relevant organizations to produce a statistical framework for measuring cybercrime.[7]

The ICCS is currently being implemented in a growing number of countries with a view to improving data on crime and criminal justice. UNODC closely monitors this implementation, which is also useful to collect feedback and suggestions on possible inconsistencies and gaps that may emerge at country level so that they can be addressed in future versions of the ICCS.

UNODC welcomes proposals on the addition of cybercrime-related crime types to the ICCS framework or adjustment to the disaggregating variables, such as expanding the scope of the cybercrime-related variable to create more specificity. For instance, the variable could distinguish between cyber-dependent and cyber-enabled crimes.

For more information and any ICCS related inquiries, please contact UNODC at:
unodc-iccs@un.org
or refer to the website:
https://www.unodc.org/unodc/en/data-and-analysis/statistics/iccs.html

[7] These discussions could follow the same logic as the ones for the construction of the 'Statistical framework to measure gender-related killings of women and girls (femicide/feminicide)', endorsed by the United Nations Statistical Commission in 2022. The framework was produced by UNODC jointly with the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), in full alignment with the ICCS. For more information, visit: https://www.cdeunodc.inegi.org.mx/index.php/statistical-framework/