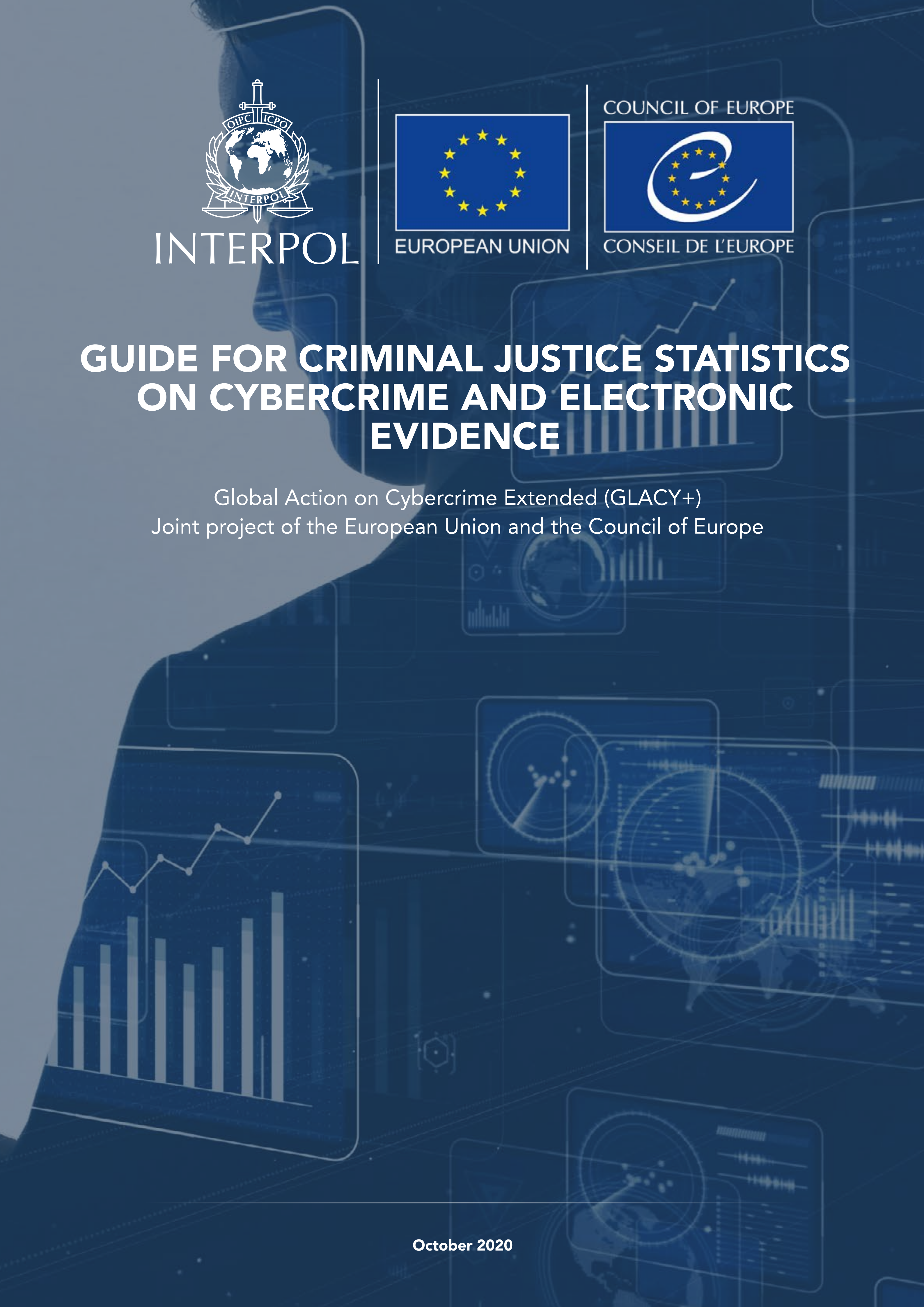

INTERPOL

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GUIDE FOR CRIMINAL JUSTICE STATISTICS ON CYBERCRIME AND ELECTRONIC EVIDENCE

Global Action on Cybercrime Extended (GLACY+)
Joint project of the European Union and the Council of Europe

October 2020

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Acknowledgement

The present *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* was prepared under the joint project of the European Union and the Council of Europe on Global Action on Cybercrime Extended (GLACY+). The work on this document was coordinated by the Cybercrime Programme Office of the Council of Europe (C-PROC) and the INTERPOL Cybercrime Directorate. Contributions were received from experts of the General Inspectorate of Romanian Police and the Korean National Police University.

Contact

Cybercrime Division
Council of Europe Directorate General Human Rights and Rule of Law
F-67075 Strasbourg Cedex (France)
E-mail : cybercrime@coe.int

INTERPOL Cybercrime Directorate
INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510
E-mail: EDPS-CD@interpol.int
Twitter: @INTERPOL_Cyber

Disclaimer

The views expressed in this technical report do not necessarily reflect official positions of the Council of Europe, of the European Commission, of INTERPOL or of the Parties to the treaties referred to.

FOREWORD

As information technology becomes widespread in our society, the crimes targeting or using computer systems have also become increasingly common. Governments worldwide are recognizing the need for action to combat cybercrime effectively on a global scale, and many countries have undertaken efforts to adopt criminal legislation and to establish specialized cybercrime units and units responsible for digital forensics in recent years.

To effectively tackle cybercrime, public authorities need a good understanding of the scale, types and impact of crime in cyberspace. However, the borderless nature of the Internet and the constant evolution of technology and techniques used by offenders, such as cryptography and the Darknet, make it difficult for criminal justice authorities to obtain a full understanding of the problem. It is therefore challenging for governments to ensure that societies and individuals are able to benefit from information technology.

In this context, the Council of Europe and INTERPOL jointly developed the present *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* to support countries in having a clearer vision of the global problem. This guide lays out the agenda for compiling criminal justice statistics with key steps for data collection, analysis and cooperation among multiple stakeholders.

Well-defined statistics produced in collaboration with criminal justice authorities will not only provide valuable insights into the changing environment, but also strategic indicators for measuring the effectiveness of policies and activities. It will also serve as a solid foundation for developing tailored operational responses to reduce the impact of cybercrime.

How countries approach cybercrime and electronic evidence at the national level has a real impact on available options on global cooperation. We call upon criminal justice authorities worldwide to join the efforts for effective international cooperation against cybercrime by collecting, analysing and sharing more transparent, accurate and consistent statistics. We believe that statistics can be a powerful tool to counter cybercrime and protect societies for a safer world.

Craig Jones
Director of Cybercrime Directorate
Executive Directorate for Police Services
INTERPOL

Alexander Seger
Head of Cybercrime Division
Directorate General of Human Rights and
Rule of Law
Council of Europe

Table of Contents

ABBREVIATIONS, ACRONYMS AND TERMS

Budapest Convention on Cybercrime, the first international treaty seeking to address crime against and by means of computers and the securing of electronic evidence by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

CERT/CSIRT Computer Emergency Response Team/Computer Security Incident Response Team

CJA Criminal Justice Authority

Collection form a document to be used as template for collecting data

Cyber-dependent crime crimes which can be committed through the use of computer system against the confidentiality, integrity and availability of computer data and systems – i.e. Illegal access, illegal interception, interference of data or systems, and misuse of devices

Cyber-enabled crime traditional crimes which can be increased in their scale or reach by use of computer networks or other information communication technology

Cybercrime category class of cybercrime activities sharing similar characteristics, especially used in cybercrime data collection form.

Cybercrime data statistically reportable information derived from recognized offences

Data reporter practitioner who transforms an empirical observation into cybercrime data

Electronic evidence (e-Evidence) evidence in electronic form

MLA Mutual Legal Assistance

Offence attributes observable/observed patterns that can be recorded as features or characteristics of an offence

Recognized offence criminal event that is brought to law enforcement attention via reporting or empirical observation by law enforcement.

EXECUTIVE SUMMARY

Statistics on cybercrime and electronic evidence allow criminal justice authorities to have a clearer view of the cybercrime phenomenon in an ever-developing technological environment. They not only allow the authorities to clearly assess crime trends, but also help to measure the efficiency of their approaches and activities.

We find diverse practices in different organizations and countries. This guide includes, among others, examples of the UK Home Office Counting Rules (HOCR), Crime Survey for England and Wales (CSEW), Scotland's Justice Analytical Service Division's multi-disciplinary analytical teams, the United States Bureau of Justice Statistics, South Korea's Information System of Criminal Justice Services (KICS), and the Australian Cybercrime Online Reporting Network (ACORN). These examples demonstrate transparency, accuracy and consistency in the collection and analysis of statistical data.

General practices by law enforcement and judicial authorities on cybercrime and electronic evidence statistics can be summarized as follows:

- Statistics on cybercrime, electronic evidence and the special tools used for its collection may help authorities in assessing the criminal trends and new technologies used by criminals.
- The structure of the record should be predefined, preferably in a collection form. Different collection criteria may be imposed reflecting national legislation and practice.
- Officials engaged in collection need to have sufficient subject matter knowledge to distinguish the patterns in observed crimes and be familiar with the collection policy.
- Judicial authorities, prosecutors and the police may agree on common collection form and share the responsibilities for collecting data.
- Alternative data sources may supplement the statistics. Such resources include the data collected from the crime reporting system, CERT/CSIRT or other relevant entities.

When developing or maintaining statistical systems, organizations should take a strategic position and constantly monitor the ever-changing conditions and apply revisions. We also recommend that they consider centralizing the data collection process, adopting common reporting methods, supporting stakeholders, building uniform statistics, and utilizing case management systems.

Statistics become even more useful when shared. The police, judicial authorities and other appropriate authorities should explore possible synergies in exchanging and correlating the data. Such cooperation should take place among national authorities and among the international criminal justice community.

1. INTRODUCTION

Measuring the impact of cybercrime enables the whole spectrum of the criminal justice system to shape effective policies and operational responses. It also allows evidence-based mobilization and alignment of resources. By analysing the figures and trends, criminal justice authorities could have a better picture of their own capacities and areas of improvement. In this context, the Council of Europe and INTERPOL have jointly developed the *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* to help countries compile statistics in an efficient manner. The main purpose of this guide is to support criminal justice authorities in introducing the statistics on cybercrime and electronic evidence by providing good practices and recommendations.

At present, there is a lack of understanding of the impact of cybercrime, which leads to numerous challenges as to how authorities set strategic goals and develop operational responses in tackling it. Often cyber initiatives are developed based only on hypothetical needs, and resources may therefore be misallocated. Therefore, the agenda related to criminal justice statistics has been attentively discussed in the law enforcement community. Within this dialogue, there is a general understanding that the statistics on crime and evidence would quantify and measure the level of threats posed by cybercrime.

Meanwhile, some criminal justice authorities who created statistics have experienced challenges in developing, implementing and interpreting. This is in part due to the absence of a common approach on the methodology for collection and usage of statistical data. There is also no consensus on how relevant authorities can integrate data at the regional or national level, and the methodology or scope of collectable data. Given the diverse systems and policies, each country is likely to develop its own methodology and categories of data to be collected on cybercrime and electronic evidence.

At the international level, the differences between countries' judicial systems makes it even more complicated. For instance, the legal definitions of crime differ between countries. In addition, the capacity or capabilities of criminal justice authorities in investigation, prosecution and adjudication in the national context could vary. In terms of sources, authorities outside the criminal justice system may also hold relevant data on cybercrime and electronic evidence. Computer Emergency Response Teams/Computer Security Information Response Teams (CERT/CSIRT) are good sources of data for accurate and relevant statistics. Therefore, cooperation with diverse actors in industry and academia can be helpful.

This guide is to be used as a reference for enhancing specialized cybercrime capabilities of law enforcement and criminal justice systems in various national contexts. Moreover, it provides recommendations on how to integrate statistics within the day-to-day operations of the criminal justice authorities. Like other statistics, the data were collected by respondents who translated experienced facts into metadata prepared by the collecting agency. The guide also limits the definition of statistics to the collection of data on actual cases from practitioners working at criminal justice authorities.

2. PRACTICES ON STATISTICAL DATA ON CYBERCRIME AND e-EVIDENCE

2.1 Regulations and Policies

Crime statistics can help develop a better and efficient understanding of crime, but they are typically not regulated or prescribed thoroughly by legal instruments. It is also difficult to find a legislative example that acknowledges such needs for cybercrime and electronic evidence. In practice, these statistics are often the bi-product of government authorities in pursuit of other initiatives.

One of the rare examples can be found in the European Union which requires its Member States to bring statistics into the functions of the governments. Article 14 (Monitoring and Statistics) of Directive 2013/40/EU on attacks against information systems stipulates that statistical systems be in place:

- Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 (Illegal access to information systems) to 7 (Tools used for committing offences).
- The statistical data shall, as a minimum, cover existing data on the number of offences referred to in Articles 3 to 7 registered by the Member States, and the number of persons prosecuted for and convicted of the offences referred to in Articles 3 to 7.

On combating the sexual abuse and sexual exploitation of children, the Directive 2011/93/EU encourages its Member States to create mechanisms for data collection at the national or local levels for the purpose of observing and evaluating the criminal phenomenon.

The 7th evaluation round (Genval[1]) conducted at EU level on the capabilities of Member States in the area of cybercrime also referred to the subject of criminal justice statistics, for which several recommendations were made as policies to be followed:

- Member States facing problems related to the lack of common definition or of common understanding of cybercrime are encouraged to develop a consistent national definition (or understanding) of cybercrime to be applied by all stakeholders involved in fighting cyber criminality and for the purpose of compiling statistics.
- Member States should gather specific statistics for cybercrime allowing both to check the overall cybercrime figures and to identify the share of cybercrime in the global criminality picture.
- Member States should develop a standardized approach to collect comprehensive statistics in the different stages of the proceedings, broken down into specific cybercrime areas, preferably those identified at the EU level, i.e. online child sexual abuse, online card fraud and cyber-attacks.
- Member States should consider solutions allowing interoperability of the various databases containing cybercrime figures, with a view to quickly achieving cases comparison, criminal identification and cases quantification.
- Member States should facilitate the exchange of statistical data among the different national authorities involved in tackling cybercrime, in particular between LEA and judicial authorities

At national level, legislations may include provisions regarding the institutions responsible for the collection and maintenance of statistical data for various areas of activity, including crimes. The legislations do not often mandate the criminal justice statistics either in general or in the cybercrime area. They are usually general provisions without details on the categories of data and periods of data collection. Whenever the legislation includes reference to statistical data to be maintained by the authorities responsible, the internal regulations of that authority would define details of the methodology.

[1] http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf

2.2 References and Good Practices

Association of Chief Police Officers (ACPO) publishes the *ACPO Managers Guide on Good Practice and Advice Guide for Managers of e-Crime Investigation* and the ACPO Good Practice Guide for Digital Evidence.[2] ACPO was replaced in 2015 by a new body, the National Police Chiefs' Council. The UK Crown Prosecution Service provides a comprehensive overview of challenges of investigating and prosecuting cybercrime.[3]

Australian Cybercrime Online Reporting Network (ACORN)[4] is an online system where people can securely report cybercrime, and find advice on how to recognise and avoid it. The national policing initiative is delivered by all Australian police agencies and the Australian government working together to combat cybercrime. Once a report has been submitted, it is assessed and can be referred to the police for investigation although not all reports can be investigated. However, these reports contribute to the national intelligence database which is a key component in the fight against cybercrime.

In Brazil, the National Public Security Information System, Prisoners, Weapons and Ammunition Traceability, Genetic Material, Fingerprints and Drugs (SINESP),[5] is an integrated information platform that allows operational, investigative and strategic public security consultations. Under the responsibility of the Ministry of Justice and Public Security, SINESP has established itself as one of the means and instruments for the implementation of the National Public Security and Social Defense Policy.[6] The system compiles national statistical information on crimes, such as rape, personal injury followed by death, intentional homicide, robbery, attempted murder, vehicle theft, cargo theft and theft from financial institutions. All statistical data are accessible to the general public.[7] However, Brazil does not have centralized official statistical data on cybercrime or cyber-enabled crime. Each Federation Unit (26 States and the Federal District) has a police force to investigate criminal offences, including those committed in cyberspace. Most of these states have cybercrime units to investigate this type of offence, notably cyber-dependent crime. Cyber-enabled crime is investigated by the police station where the victim reported the incident. Most of the time, these reports are considered as common crime. There are differences in the way of collecting and accounting for statistics according to the Federation Unit. In situations where the attribution to investigate these crimes is the responsibility of the Brazilian Federal Police,[8] the statistical data related to cybercrime are extracted from the National Criminal Information System and are determined in relation to cyber-dependent crime. Cyber-enabled crime is recorded in relation to the act typified as a crime but not the means used in execution of the crime. The e-evidence is registered in the National System of Forensic Management, which obtains statistics of all evidence analysed by the Brazilian Federal Police, whether it is cyber-dependent crime or cyber-enabled crime.

In Canada, Statistics Canada[9] is responsible for reporting on the nature and extent of crime as well as the administration of criminal and civil justice in Canada. These statistics come within the scope of the following objectives of the justice system: public order, safety, and national security through prevention and intervention; offender accountability, reintegration, and rehabilitation; public trust, confidence,

[2] http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (last accessed 6-April-2017)

[3] http://www.cps.gov.uk/legal/a_to_c/cybercrime/index.html (last accessed 6-April-2017).

[4] https://www.acorn.gov.au/

[5] http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12681.htm

[6] http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13675.htm

[7] Published statistics: https://www.justica.gov.br/sua-seguranca/seguranca-publica/sinesp-1/bi/dados-seguranca-publica

[8] Especially in criminal offences committed to the detriment of goods, services and interests of the Union or its autonomous entities and public companies and in those whose practices have interstate or international repercussions and requires uniform repression: http://www.pf.gov.br/institucional/acessoainformacao/institucional/competencias

[9] http://www5.statcan.gc.ca/subject-sujet/theme-theme.action?pid=2693&lang=eng&more=1(last accessed 6-April-2017)

and respect for the justice system; and social equality and access to the justice system for all citizens and serving victims' needs.

The European Network and Information Security Agency (ENISA) publishes a *Good Practice guide on Cooperative Models for Effective Public Private Partnerships.*[10] This guide classifies Public Private Partnerships (PPPs) for security and resilience and reveals the main five components addressing why, who, how, what and when questions associated with creating and maintaining PPPs. The guide collects data from both public and private sector stakeholders across 20 countries. There is also a separate report on *Electronic evidence provides a basic guide for First Responders.*[11] This report offers guidance for CSIRTs on managing and gathering evidence, including the collection of statistically relevant data.

- In 2016, ENISA published a good practice guide on using taxonomies in incident prevention and detection.[12] It provides conclusions and recommendations on improvements that can be made on current cyber incident taxonomies.
- Given the differences between EU Member States in terms of common definitions, standardized instruments and methodology for collection of statistical data, which resulted in limited comparability of crime statistics among the countries, an EU guidelines was issued in 2017.[13]

In the Republic of Korea, the Korean national police collects data from its regional police branches via the integrated information systems called Korea Information System of Criminal Justice Services (KICS). It was established under the legislation mandating the use of IT systems in all criminal justice procedure for transparency and efficiency.[14] The courts, Ministry of Justice, the Prosecution Service and the police must use a standardized data table to proceed with investigation, prosecution, trial, and enforcement. The end user interface of this system is the case management system used by individual public officials including police detectives, case prosecutors and judges. New cases and arrests are entered into the system from police detectives working at 255 police stations under 18 regional police agencies. The case documents such as victim's report, suspect interview, forensics report, warrants and any obtained data, and police observation reports are electronically attached to these case files. The statistics are published to the public under 467 different crime categories.[15] Case metadata includes time, place, modus operandi, tools, accomplices, damage, among others. Suspect metadata includes socio-demographic elements such as age, gender, occupation, living standard, marital status, family details, educational background, mental illness, nationality, criminal record, hideouts, accomplices and past use of drugs. Statistics are first collected at the time of receipt of the report (case statistics), interviewing or during the investigation process (suspect statistics), mainly by the police officer in charge of the case. Data can be added by other officers, the case prosecutors and judges as the cases move toward the court.

In the United Kingdom, the Home Office publishes *Home Office Counting Rules* (HOCR).[16] Crime is recorded by the police and others to: ensure that victims of crime receive the service they expect and deserve; prioritize effective investigation of crime in keeping with national standards and the College of Policing's Code of Ethics; inform the public of the scale, scope and risk of crime in their local communities; allow Police and Crime Commissioners (PCCs), Forces and local partners to build

[10] https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps

[11] https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders

[12] https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection

[13] https://ec.europa.eu/eurostat/documents/3859598/8305054/KS-GQ-17-010-EN-N.pdf/feefb266-becc-441c-8283-3f9f74b29156

[14] South Korea's Act on Promotion of the Digitalization of the Criminal Justice Process, 25 Jan 2010 (https://elaw.klri.re.kr/kor_service/lawView.do?hseq=45472&lang=ENG)

[15] Published statistics at KNPA (https://www.police.go.kr/eng/statistics/statisticsSm/statistics04.jsp)

[16] https://www.gov.uk/government/publications/counting-rules-for-recorded-crime (last accessed 6-April-2017) (last accessed 6-April-2017)

intelligence on crime and criminal behaviour necessary for an efficient and effective response; enable Government, PCCs, Forces and their partners to understand the extent of demands made on them and the associated costs of service delivery; and inform the development of Government policy to reduce crime and to establish whether those policies are effective.

Crime Survey for England and Wales (CSEW) added new questions on fraud and computer misuse in October 2015. These questions have now been included within the CSEW for a full 12 months, with sufficient data having been gathered to form a new additional headline estimate of total CSEW crime. This estimate and others on fraud are produced as Experimental Statistics.[17] Experimental Statistics on fraud and cybercrime recorded by the police are also published including: Action Fraud data at police force area level, based on victim residency; and, police recorded crime data on offences that were considered as having an online element.[18]

In Scotland, statisticians within the Justice Analytical Services Division, [19] work within two policy-focused, multi-disciplinary analytical teams which include social researchers, economists and performance analysts. The teams provide statistical information and support relating to police and community safety, court affairs and offenders, prisons and matters relating to civil and international law.

- The Justice Analytical Unit provides analytical advice and support in the areas of both criminal and civil justice, working with a range of key stakeholders to develop a shared understanding of available evidence and to maximize the use and impact of this evidence across the justice system.
- The Safer Communities Analytical Unit works closely with a range of external stakeholders, including Police Scotland, the Scottish Police Authority, and the Scottish Fire and Rescue Service, to develop a shared understanding and promote use of the available evidence.

In the United States, the Department of Justice, Bureau of Justice Statistics,[20] established in 1979, collects, analyses, publishes and disseminates information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government. These data are required by federal, state, and local policymakers in combating crime and ensuring that justice is both efficient and even-handed. The FBI Uniform Crime Reporting (UCR) Program[21] was conceived in 1929 to meet the need for reliable uniform crime statistics for the nation. In 1930, the FBI began collecting, publishing, and archiving the statistics. Data was received from over 18,000 city, university/college, county, state, tribal, and federal law enforcement agencies voluntarily participating in the program. These data are used to generate four annual publications: Crime in the United States, National Incident-Based Reporting System, Law Enforcement Officers Killed and Assaulted, and Hate Crime Statistics. The crime data are submitted either through a state UCR Program or directly to the FBI's UCR Program.

The United Nations Office on Drugs and Crime (UNODC)[22] produces and disseminates accurate statistics on drugs, crime and criminal justice at the international level. UNODC also works to strengthen national capacities to produce, disseminate and use drugs, crime and criminal justice statistics within the framework of official statistics. It develops a number of statistical standards and recommendations in the field of crime, criminal justice and illicit drugs in collaboration with national authorities and relevant international organizations. The objective is to enhance the comparability of

[17] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/year-endingdec2016#what-has-changed-within-this-publication

[18] An offence is flagged where the reporting officer believes that on the balance of probability, the offence was committed, in full or in part, through a computer, computer network or other computer-enabled device.

[19] http://www.gov.scot/Topics/Statistics/Browse/Crime-Justice (last accessed 6-April-2017)

[20] https://www.bjs.gov/index.cfm?ty=abu (last accessed 6-April-2017)

[21] https://ucr.fbi.gov/ (last accessed 6-April-2017)

[22] https://www.unodc.org/unodc/en/data-and-analysis/statistics.html

statistics at international level and to support countries in their efforts to produce national statistics on drugs, crime and criminal justice.

Although many good practices can be identified on a national level, very few platforms collect and publish standardized, reliable statistics on cybercrime on the global level. In this context, INTERPOL, as a global and neutral organization, aims to aggregate cybercrime data and statistics globally utilizing its Cyber Analytical Platform. It will then develop a more accurate threat assessment on a global scale and provide tailored operational support to its member countries.

When producing and disseminating crime and criminal justice data, it is important to understand the general statistical principles. Collected data need to be transparent, accurate, and consistent. A central national collection point can support quality control and interagency cooperation as well as evidence based policy changes.

3. COLLECTION OF STATISTICAL DATA ON CYBERCRIME AND E-EVIDENCE

3.1 Law Enforcement Practices

As part of their responsibilities, the police units collect and maintain statistical data, mainly for the purpose of assessing two relevant aspects:

- Trends/evolution of crime;
- Efficiency of the activities performed by the police units for a specific crime area and for a limited period of time.

Initially, data are collected at the local or regional field offices, then forwarded to the central office for further integration. Using a standardized form at both regional and central level would ensure the assessment of the crime. In order to have proper crime assessment throughout the statistical data, it is necessary to have predefined criteria and periods of time set in advance.

The structure of statistical data on crime must include the most relevant criteria on the criminal activities to be assessed, such as offences, cases, persons, victims, prejudice, status of the investigation, measures taken, punishment, evidence, goods seized, finalization, etc. to achieve the objectives envisaged by the statistics. These criteria should be developed into a predefined form for collection. The form used for the collection of statistical data should be constantly monitored to adjust any discrepancies with field practices, evolution of crime, changes in legislation, or to add or remove specific features of the statistics.

It is important for the producers as well as the consumers of the statistics to have a common linguistic understanding of the criteria and the terms in the collection form. To enhance the coherence, it is recommended to train the staff involved in the collection and processing of statistical data. The collection of statistical data requires sufficient knowledge and experience in crime and processing the data.

Collection and processing of statistical data at the central level varies according to the organizational structure of the police units and the purpose. The periods when the statistical data are collected and processed may differ according to the purpose they serve, specificity of judicial systems, and envisaged type of crime.

3.1.1 Cybercrime statistics

Collection and use of statistical data

In the area of cybercrime, the criteria for collection of statistical data may differ from other crime areas, mainly due to:

- Transnational character of cybercrime and the need to use international cooperation channels during the investigation;
- Offenders and victims could be from different jurisdictions;
- Use of technical devices for conducting the criminal activity and the need to seize and exam such devices;
- Use of electronic means of payment in the criminal activity;
- Use of specific instruments for the collection of electronic evidence during the investigations;
- Intensive use of electronic evidence to prove the criminal activity;
- Specificity of various cybercrimes cases (computer fraud, computer attacks, child sexual exploitation through computer systems, etc.).

The following data are recommended to be collected and outlined as being relevant for drawing a clear picture of the criminal activity:

- Cases initiated, under investigation, or solved;
- Cases under the supervision of prosecutors or subject to the competence of prosecutors;
- Reported/identified offences;
- Identified suspects (age, sex, nationality, etc.);
- Measures applied (custody/arrest);
- Investigative powers (interceptions, surveillance, authorized computer access, etc.);
- Locations searched;
- Victims identified (age, sex, nationality, etc.);
- Damage incurred (preferably, as value in money);
- Assets seized (by type, category and value).

An accurate status of cybercrime could be generated by statistical data kept by the types of cyber offences as provided in national legislation.

Keeping statistical data separately by types of cybercrime may identify the trend of certain forms of cybercrime or the geographical area where they are more intense. This will help authorities better allocate their resources and efforts to ensure a more appropriate and efficient response.

The effectiveness of the activity of police units in the area of cybercrime may also be assessed as an analysis of indicators showing the outcome of the investigation, such as cases solved, measures taken, seized assets, and suspects identified. The collection of statistical data in the field of cybercrime requires the fulfilment of two main prerequisites: the existence of legislation specific to cybercrime, and police units specialized in cybercrime.

Reported offences

The reporting of crimes is crucial for police units in understanding and analysing cybercrime. The data collected through reporting systems is useful for producing statistics, entering in databases, and initiating investigations. When complemented with other crime related data from other police units, it may help generate more precise and complete statistics.

The reporting mechanism may differ from police to police and can include telephone lines, e-mail addresses, web platforms, fax, etc., reachable by anyone willing to report criminal activities. It can be collected at the local, regional, or national levels. It also can be general or specific for some types of offence.

For cybercrime offences, it is recommended to have in place a dedicated reporting system, adapted to the nature of such crimes, as they involve the online environment and transnational elements. The existence of an online reporting system dedicated to cybercrime allows easy access to anyone who wants to file a report, which might involve a different jurisdiction.

Furthermore, police units together with the private sector may develop a common reporting system in order to increase the trust of the people willing to report, and offer guidance and support for them. A relevant example is the hotline dedicated to online child sexual exploitation, where reports about criminal activities are received and at the same time assistance or advice is offered to potential victims, contributing to the prevention of crime.

3.1.2 Electronic evidence statistics

The statistics on electronic evidence are useful in conducting criminal investigations and assessing criminal trends as well as the use of new technologies in committing crime.

In practice, relevant legislation is required. Legal instruments should provide solid grounds for the collection and handling of electronic evidence in criminal investigations and proceedings.

The two statistical elements of electronic evidence are special investigative instruments used and digital devices analysed. They are mainly linked to the organizational practice of the specialized units which deal with electronic evidence. Such units, with competencies, could help maintain statistical data. The absence of such specialized units might result in an inconsistent approach to the collection of statistical data, preventing a centralized inventory of electronic evidence, and it would be difficult to properly assess the impact of electronic evidence on criminal investigations and proceedings.

The units specialized in handling electronic evidence can be independent from or integrated in the specialized cybercrime units. When they are part of the specialized cybercrime units, their competencies in handling evidence are helpful for cybercrime investigation or assisting other police units in this area.

For producing statistical data of electronic evidence, the following types of data may be considered with some variations:

- number of cases involving electronic evidence;
- types of offences for which the electronic evidence is used;
- categories and amount of analysed storage devices or computer data;
- amount of electronic evidence analysis requested by other institutions (police/prosecutor/court);
- number of challenged/re-examined storage devices.

An important aspect is how the electronic evidence were obtained and what special investigative instruments have been used in this process. For instance, electronic evidence may be obtained directly as a result of a request submitted to the providers in the form of preservation orders and production orders (e.g. access logs, operation logs). Other evidence could be produced by analysis performed (live data acquisition and digital forensic analysis). These categories of data regarding electronic evidence should complement the ones mentioned above in the process of collecting statistical data on electronic evidence.

3.2 Judicial Authorities Practices

Rules on the organization and responsibilities of judicial authorities may support the collection and maintenance of statistical data. Prosecutors' offices, courts, and the justice department may produce some statistical data for their daily operations. At the prosecutorial level, data may be about stages of investigations, instruments and final results of cases. The courts may keep statistics on the adjudicated cases, sentences, and measures ordered.

The main source of statistical data for the justice department is also the courts. The data are used to carry out surveys or evaluations of crime, punishments or sanctions and identifying the need to amend the existing interpretation of the law.

Compared to the statistics collected by the police, which usually reflect case facts, the statistics maintained by judicial authorities are more about the judicial interpretation and opinions about the facts and final conclusion of the investigation.

3.2.1 Cybercrime statistics

At the prosecutor's office, the following categories of data can be considered for cybercrime statistics:

- Number of cases directly reported or transferred from the police units;
- Number of prosecutions conducted;
- Number of people investigated/prosecuted;
- Number of victims;
- Status of prosecutions and measures ordered;
- assets seized;
- Damage incurred;
- Final solutions (indictments, cases sent to the court, cases closed, cases sent back to the police, etc.)

Similar to data collection by law enforcement, a well-defined collection form may increase the value of statistics. It can be adjusted according to the needs of specific types of cases or criminal areas. The police and prosecutors could agree upon a single unified collection scheme, where police provide factual information about the criminal case as they operate, and the case prosecutor would later add the subsequent legal assessment. Such unified case management is not only useful in statistical data collection, but also increases transparency and accountability of the opening and closure of criminal cases at police level.

It is crucial that personnel in charge of the collection and processing of statistical data be properly trained to understand the necessary protocols related to their collection.

The courts may have difficulties in collecting data for cybercrime statistics. They could extract factual data from adjudicated cases, but the number of adjudicated cybercrime cases is relatively low to understand the general phenomenon. Rather than focusing on factual data collected by law enforcement, courts should record how they assessed the case: legal instruments used and types of evidence admitted or rejected.

In particular, the courts may provide important information on cybercrime cases. It is beneficial for both police and prosecutors to follow up on the results of cases in the courts to assess and improve their statistical data on:

- Use of investigation instruments;
- Assessment of evidence, including electronic evidence and described facts;
- Solutions and justification.

3.2.2 Electronic Evidence Statistics

The electronic evidence presented by the police and prosecutors is assessed at the court, and the result can be included in the statistics. The court's opinion can provide valuable feedback to the investigative authorities who handled the evidence. An integrated system for statistics would provide law enforcement with feedback on the usefulness of evidence at the level of courts related to the cases initiated by them.

Judicial authorities also perform safeguard roles in collecting and analysing electronic evidence. Depending on legislation, the investigative activities to obtain or analyse the evidence such as preservation, production, interception and computer forensic analysis, may need to be authorized by judicial authorities. As a result, the statistical data of legal instruments used to obtain electronic evidence exist as long as the legislation provides them and there is interest in assessing their usefulness in investigations and prosecutions.

3.3 Practices of non-criminal justice actors

3.3.1 CERT/CSIRT

In the process of preventing and fighting cybercrime, certain responsibilities also belong to CERT/CSIRT entities. Although they are not law enforcement agencies and their responsibilities mainly concern cybersecurity, CERT/CSIRT entities may cooperate with enforcement agencies and other relevant private entities.

Regardless of the differences in the organizational structure of CERT/CSIRT and their responsibilities, they are able to collect and process specific types of data in relation to cybercrime as follows:

- Number and types of cyber incidents;
- Number and types of cyberattacks;
- Targeted computer infrastructure;
- Sources of cyberattacks;
- Envisaged security measures;
- Instruments used in carrying out attacks;
- Reports sent to law enforcement agencies.

The data maintained by CERTs/CSIRTs can support the understanding of crime and the evolution of trends as well as the decisions for taking adequate security measures.

The data collected by CERTs/CSIRTs can also help law enforcement agencies to identify criminal threats with the aim of improving their approach and identify solutions for inter-agency cooperation.

3.3.2 Cybersecurity industry

The ecosystem of the Internet industry is becoming more diversified and complex. The cybersecurity industry plays an important role in defending individuals, industry and infrastructure. Security vendors focus on users, IT devices, network, data, application or entire enterprises to provide commercial solutions to detect and respond to cyber threats.

Many vendors collect data as part of their business, and publish some of the useful findings generally in the form of periodic reports. Examples of such data include:

- Number of detected threats by type, geographical region, profile of victims, etc.;
- Financial impact of the threat;
- Response time related to the vendor's service.

The data may be collected from the subset of their customer base. Ultimately, these reports could support law enforcement in understanding cybercrime for both criminal investigation and policy making.

3.4 International cooperation statistical data

3.4.1 Police-to-police cooperation

International cooperation among police organizations is crucial when it comes to investigating transnational crime. Investigating cybercrime, a great volume of information and data is exchanged among different jurisdictions. Some of the data can later be used in court and some of the information can become important evidence. Such exchange of data and information is the responsibility of law enforcement, which has specialized cooperation units and channels.

The activity of international cooperation at the police level can be made into statistics by: the number of requests for cooperation received/sent, types of information requested, and police channels used for cooperation (INTERPOL National Central Bureaus and I-24/7, Europol, liaison officers, direct contact). This statistical data may be held separately by the cybercrime units, and may help in assessing criminal trends and evaluating the relevance of the transnational elements.

Information shared through police-to-police cooperation can potentially be used as evidence in the requesting country. The types of data that one police force would share with another may vary among countries due to local legislation and law enforcement culture. Many police would share details of Internet Protocol (IP) addresses, basic user information and other voluntarily obtainable data. They would refrain from sharing information that can be better pursued under legal assistance, where safeguard measures are required to protect the information.

3.4.2 Mutual Legal Assistance

The authorities responsible for issuing or executing international mutual legal assistance (MLA) requests, including the exchange of evidence, are in general the prosecutors' offices.

The categories of data that may be included in statistics about international cooperation on cybercrime are:

- Number of requests (MLA) sent/received;
- Types of offence envisaged;
- Types of check requested to be performed;
- Types of measure requested to be taken;
- Electronic evidence (number, type, etc.);
- Number of joint investigations performed;
- Number of extradition requests;
- Number of requests for the case to be transferred.

The collection and maintenance of statistical data concerning international cooperation on cybercrime, with regard to MLA requests, could highlight the number of requests and the need for development of capabilities such as institutions, channels and instruments for international cooperation.

3.4.3 Preservation requests

One of the international legal standards on cybercrime is the Budapest Convention, which includes provisions for international cooperation. This instrument concerns the preservation of stored computer data requested by a country from another country, aiming to avoid losing it from the network, taking into consideration its volatility. The data can be subsequently sent to the authorities of the requesting country only after receiving the request through the appropriate cooperation channels. This instrument ensures rapid communication between the authorities from different countries and makes it possible to preserve evidence until the submission of the request through official channels.

Preservation requests could be submitted through 24/7 contact points established according to the Budapest Convention as part of police, prosecutors' offices or other competent authorities.

The statistical data for preservation requests could include the following information:

- Number of preservation requests received/sent (by country);
- Categories of computer data envisaged;
- Types of offence for which preservation requests are made;
- Number of preservation requests followed or not by MLA.

The maintenance of such statistical data is helpful for the assessment of the cooperation instrument and the resources allocated to process and execute preservation requests.

4. RECOMMENDATIONS FOR DEVELOPING STATISTICS

4.1 Strategic Approach

A safer road to success in compiling statistics is by setting a strategic goal and implementation plans. While respecting its current strategy and guiding policy, an organization needs to find a proper structural position in which the strategic plan can be reflected. If the organization already has a structured strategic framework or strategic plan, it could start as an independent project.

4.1.1 Setting Strategic Objectives

Defining the objectives or goals is a crucial element of the roadmap. Effective goals statements are specific, measurable, achievable, relevant, and time-bound (SMART). Below are a few high-level principles in the compilation and dissemination of criminal justice statistics:

- Transparency, accuracy, consistency;
- A central national collection point that can support quality control and inter-agency coordination;
- Evidence-based policy making.

Despite different methods in setting goals, it should follow the existing culture and guiding policies of the organization, engaging the organization's leaders and visionaries in the process. Like any element in strategic planning, the objectives or goals are fluid and can change at any stage.

4.1.2 Environmental Scanning

The next task is to understand the environment and assess the organization. In order to evaluate the organization's regulation, culture, management style, human resources, information systems and financial resources, the following questions could be asked:

- What reporting structure do you have, and can it be used for data collection?
- What makes it easy to collect and aggregate data and what can go wrong?
- Is it easy to introduce internal regulation, or is there strong management support?
- Are there similar attempts to categorize cybercrime or electronic evidence? What went well/wrong?
- Are there other initiatives to join efforts – projects on IT, training, legislation, etc.?
- What is the root cause of any challenge?

There are several tools and approaches available that can analyse the internal or external environment and build the strategic framework.

4.1.3 Monitoring the plan

Once objectives and action plans have been defined, it is important to include the organization's management and key persons, staff who will perform duties when the plan is to be implemented. Developing a common understanding of the goal and methodologies is also essential throughout the development and implementation of the strategy.

Documenting the plan is useful as it is being developed in group efforts. It can start from analysis of the organizational situation, current guiding policy, goals and actions, as well as logical reasons for how the actions can lead to the goals.

4.2 Implementation Key Points

Within the boundaries of the strategic approach, the actions below are generally applicable in developing a strategic approach on cybercrime and electronic evidence statistics.

Centralized system for collecting statistics

It is broadly accepted that the collection and submission of statistics requires dedicated resources. These resources could be located in every agency and organization that is responsible for their collection, but it is more efficient and effective if this role is integrated in a centralized system.

In all cases, there will be a need to share data in order to perform effective analytics. A centralized system is a more cost effective and efficient strategy. Data should be collected from the local, regional and national levels and integrated based on common criteria.

Common reporting methodology with broad stakeholder support

Agreed proposals for common reporting supported by written guidelines for cooperation between authorities and private sectors will enhance the value of the data collected. Issues related to cross-border cooperation on cybercrime investigations and electronic evidence will also need to be addressed.

Uniform statistics with clear definitions

Uniform statistical definitions will initially take significant effort to create but can define what specific data is collected and who will be responsible for collecting these data in a regular and timely manner. Within a country, police - prosecutors - judges may agree upon the unified crime data scheme and take shared responsibilities for collecting and consuming data.

Case management system

A number of countries have already adopted case management systems to maintain records relating to investigations and provide tracking and progress supervision on active cases. These systems provide a central repository for all investigations and are used to record and generate statistics which can be shared with other stakeholders while maintaining appropriate secrecy and confidentiality. A statistical management system is required for the management of data collected for analysis to avoid fragmented statistics from different institutions.

This will also track cases throughout the entire process, from reporting, investigation, prosecution and adjudication, with the result of accurate statistical data.

Clarity in the definition of cybercrime

Many countries have complex systems for criminal justice statistics, but few countries have protocols for statistics on cybercrime and electronic evidence. Many traditional and widely understood crimes in the ‘physical world’ are now also committed by using computer systems, and do not necessarily appear as such in crime statistics.

Other offences – in particular offences against computer systems and data – may be more clearly defined in criminal law but may only be a secondary element in a larger criminal investigation.

In short, much cybercrime is underreported or overlooked when it comes to keeping data and maintaining statistics on trends associated with cybercrime. Therefore, it is important to clearly determine how cybercrime is defined or categorised for statistical purposes.

4.3 General steps for data collection

The methodology for data collection could include the following five main phases, which are relevant for the preparation and use of cybercrime statistics:

Identify data sources

Identify all reliable sources of data according to the local context and legislation. It is important to involve all stakeholders and to define requirements regarding the data to be collected. The data should then be collected, possibly by one centralized unit on the national level. Following collection, the procedures for processing need to be defined such as security, data protection issues, confidentiality, etc. Data validation and consistency is also essential.

Select categories

Develop a method for categorizing crimes and data collected to avoid duplication, include all reports, and validate data. Two approaches can be adopted to define categories: by technical description of the different crimes, or using the definition of criminal offences in the national criminal code. While the former ensures a more accurate description of a single crime area that is being measured, the latter is preferable as it ensures more stability over time and, above all, comparability at the international level. Thus, the results can be compared over time as well as between countries.

Data analytics

Use data analytics to develop indicators that could measure the current state of cybercrime and support the analysis of criminal justice capacities. This process also helps identify errors and gaps. For the analysis, it is relevant to set criteria such as period, types of crime, total number of crimes, average number of crimes and crime distribution (region, gender, type of offender, type of victim). It is also useful to identify changes since the previous analysis, including trends, and to investigate possible bottlenecks.

Communication and reporting

Create aggregated reports on the basis of predefined requirements established by criminal justice authorities. It can define the relevant disclosure levels, and present data in different ways for different media sources and target audiences (media, management, politicians, children, etc.). It is also helpful to employ modern methods of communications.

Evidence Based Policy

Compare the aims and objectives of published strategies and policies against data collected over longer periods of time to determine levels of effectiveness and possible areas for improvement. It can feed the aggregated data back to the policy makers to improve effectiveness of limited resources or gaps in policy or legislation. This could assist in developing and implementing a sound plan of public initiatives, targeting the most critical areas identified in the analysis of national statistics, such as prevention and awareness raising campaigns.

4.4 Sharing of statistical data

The police, judicial authorities and all other relevant authorities should establish and maintain statistics according to their responsibilities and needs to assess the activities they perform.

The correlation and exchange of statistical data between competent agencies offer an accurate image of cybercrime and investigations throughout their process from initiation to the end.

The police keep statistics on various crimes to cover the investigation stage. Therefore, if other competent institutions (prosecutor's offices and courts) do not exchange data, it would be very difficult to complete their statistics with data on the progress of cases in the course of criminal proceedings.

The correlation of statistical data of the police with those from prosecutors' offices, for investigation and prosecution stages of cases, can be achieved and facilitated through harmonization of data categories/form and periods of collection of statistical data, as well as the periodic exchange of data between institutions.

Correlation and exchange of statistical data between police and prosecutors support the coordination of efforts in fighting cybercrime, allowing the complete assessment of the criminal phenomenon (cases, investigations, authors, victims, etc.), from the police responsibility to the prosecutor's task.

Statistical data from courts are useful in completing the information on the cases initiated by the police with the final results. The exchange of statistical data or the pursuit of the cases at the level of courts can contribute to the improvement of the work of the police and prosecutors.

4.5 More Considerations

The proposed model envisages a continuous cycle where each phase evolves as experiences and knowledge evolve. The model is designed for those institutions responsible for criminal justice statistics. It is advisable for the countries to define concrete processes and responsibilities at the national level clearly in writing.

In order to provide an initial starting point for categorizing reports, draft template tables could be defined on the basis of the categories of criminal offences foreseen in the Budapest Convention. Each of these offences is usually translated into the national criminal code in locally defined categories of crimes, which should be the ones used for collection of criminal justice statistics.

5. CONCLUSIONS

The aim of this guide is to enhance the capability of criminal justice authorities to better understand, measure and address cybercrime through the use of statistical data. It presents measures that law enforcement and judicial authorities can adopt to collect, process and maintain statistics on cybercrime and electronic evidence.

Taking a strategic approach and building an implementation plan are crucial for accurate statistics. Statistics will provide criminal justice authorities with a clear picture of cybercrime and electronic evidence and will permit them to address these challenges. Statistics can assist policy makers and regulators in making evidence-based decisions, thus enabling better policing and transparency.

An effective statistics system may be summarized as a unified statistical system encompassing relevant criminal justice authorities and stakeholders. A significant amount of communication would be needed to bring these entities together.

Aligning domestic legislation on offences, procedural powers and international cooperation on cybercrime with international standards, such as the Budapest Convention on Cybercrime, helps provide a common understanding of the conduct constituting cybercrime and thus to aggregate and compare data across jurisdictions.

The Council of Europe and INTERPOL will continue to cooperate in this endeavour and stand ready to support criminal justice authorities worldwide in view of effective international cooperation against cybercrime. Establishing transparent, accurate and consistent statistics is a key element of this common effort.

- - - - -

INTERPOL

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime
interpol.int