GLACY+

Global Action on Cybercrime Extended
Action globale sur la cybercriminalité élargie

April 2017

GLACY+
International Workshop
on Criminal Justice Statistics
on Cybercrime and Electronic Evidence

Accra, Ghana
29-31 March 2017

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

Contents

Contacts
Cybercrime Programme Office of the
Council of Europe (C-PROC)
Bucharest – Romania

Manuel DE ALMEIDA PEREIRA
Tel +40 21 201 7832
Email manuel.pereira@coe.int

Matteo LUCCHETTI
Tel +40 21 201 7830
Email matteo.lucchetti@coe.int

About GLACY+
The EU/COE Joint Project on Global Action on Cybercrime Extended (GLACY+) is to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area, while assuring compliance with international human rights standards and the rule of law. It has a duration of 48 months (March 2016 – February 2020) and a budget of EUR 10 million. It is largely funded by the EU's Instrument for Stability (IfS) with co-funding by the Council of Europe.

1 Introduction

1.1 Background and justification

Statistics on cybercrime and electronic evidence are essential to quantify the level of threats posed by the different forms of cybercrimes and cyber-enabled crimes, to support more efficient investigations and prosecutions, and to better inform strategic decisions of policy-makers and regulators. In addition, analysis of figures and trends allow criminal justice authorities to have a better understanding of their own capacities and performance to deal with cybercrime and electronic evidence.

In this regard, the assessments of GLACY+ countries conducted during the inception phase of the project pointed out common aspects of potential criticality in procedures that have been currently put in place to collect statistics on cybercrime and electronic evidence, such as: partially accessible or non-functioning reporting systems, poor collection and collation of data, inadequate management, misinterpretation of data protection issues, weak application in the policy-making cycle.

All of these issues could mislead and undermine the efforts of the criminal justice system to reduce the level of threat and harm caused by criminal behaviour, therefore it is crucial to address them via a structured discussion, which could result in a concrete roadmap for implementation of improvement actions to be undertaken by each country.

1.2 Expected outcome

Carried out under Objective 3, Result 1 of the GLACY+ project (Assessments of criminal justice capabilities), the activity builds on preliminary results obtained in the same field under the GLACY Project, and it is expected to provide advice to priority countries on systems for the collection of criminal justice statistics and other methods to monitor the performance of criminal justice capacities regarding cybercrime and electronic evidence.

By the end of this three-day workshop, the participating countries will have concluded:

- A benchmark of the systems in place to report and record cybercrime and cyber-enabled cases, as also compared to international best practices;
- An analysis of the current issues in the collection of reliable statistics and in their use to monitor the performance of criminal justice capacities regarding cybercrime and electronic evidence;
- An analysis of sources of statistics, reliability of data and methods of analysis, and how these affect criminal justice policies;
- Advice on a methodology to implement improvement actions and a roadmap of in-country activities related to the subject.

1.3 Participants

Participants included criminal justice professionals involved or potentially involved in collecting, collating and interpreting statistics for offences of cybercrime or for other offences involving electronic evidence.

These include cybercrime investigation departments or other relevant law enforcement offices, prosecution services, national CERTs/ CSIRTs, as well as any other officials considered relevant to the scope of the mission.

1.4 Related work

Since the launch of the Global Action on Cybercrime Project (GLACY) in 2013 and the subsequent GLACY+ in 2016, much has been written about the need for enhancement of recording of cybercrime criminal justice statistics. It is evident that all member countries have made some improvements in this regard, but this has been fragmented and the collation and sharing of vital statistical information has only developed to a small degree.

Recent GLACY+ country assessments highlight the need for a shared methodology to assist each country to identify the statistics available to them, appoint a central body to collate and to effectively disseminate reliable information. Each country is unique, and it is unlikely that 'one size will fit all'; however, the development of firm methodologies and standardised reporting mechanisms will assist each member country to improve domestically and be in a stronger position to share relevant information internationally.

2 Day 1

The morning started with an opening event and welcome address, support and gratitude being expressed by the host and attending dignitaries. The media were present, and much publicity material was captured during the opening address.

The first session was delivered by the representatives of the Council of Europe who provided a useful overview of the requirements for improved reporting systems for criminal justice statistics in the GLACY+ countries. The main factors that hinder the collection of reliable statistics within the GLACY+ countries have been discussed:

- Lack of common understanding of 'cybercrime' within criminal justice;
- Lack of cybercrime legislation in some of the countries;
- The absence of recording statistics in many departments;
- Limited technical capabilities;
- International cooperation still not fully functioning.

The main aims of the Council of Europe in respect of the previously identified issues rely on the strengths and wide applicability of the Budapest Convention on Cybercrime and highlighting the 'open issues' relating to Cybercrime Reporting systems and criminal justice statistics.

2.1 Country reports

A tour de table followed amongst the participating countries to share their respective situation in relation to cybercrime reporting and recording of criminal justice statistics, in terms of how data are currently gathered, analysed and used.

2.1.1 Ghana

a. Cybercrime Reporting Systems

Currently no formal national statistics are collected by the Law Enforcement Agencies detailing the number of cybercrimes reported and that are investigated by authorities. Additionally, under reporting of cyber-attacks by victims, make it difficult to compile accurate figures to ascertain the scale of the problem and the effectiveness of the country's response.

b. Institutional framework and entities involved in collection of data and statistics

The presentation from representatives of Ghana highlighted the large number of state and private organisations which record varying levels of crime-related statistics. These systems are primarily manual and are not shared with any central authority.

c. Current practices, issues and challenges

Ghana's main challenges are:

- No standardised or structured format for data reporting;
- No case management system for data collection and analysis;
- Inaccurate data capturing due to human errors in manual data entry;
- Victim unwillingness to report cybercrime incidents;
- Lack of awareness of some of the cyber laws amongst the law enforcement personnel. Inappropriate charges preferred;
- Lack of clear definition of cybercrime and distinction between cybercrime and other cyber-based malicious acts;
- Lack of visibility of the CERT-GH reporting mechanism on Portal;
- Lack of response from constituencies when alerts and advisories are sent to them.

Steps are being taken to address these issues, and they are planning to improve on (and develop) the following, going forward with the assistance of the Council of Europe:

- Implementation of Centralized Case Management System;
- Consolidation of Crime statistics forms to eliminate duplication;
- Continuous training of Criminal Justice System personnel on the effective ways of collating statistics, as well as on sensitizing them on the need for it.

2.1.2 Dominican Republic

a. Cybercrime Reporting Systems

The presentation provided a graph to illustrate the number of cybercrime complaints and the number that have been resolved. This showed impressive figures for 'effectiveness' of 90%, 89% and 99% for the following classifications, respectively:

Crimes against Confidentiality, Integrity and Availability of data, content crimes and crimes against Telecommunications. Unfortunately, the period of time involved and the methods of resolution were not clear.

Forms of public/private partnerships are in place, which make use of Law Enforcement Reporting System platforms.

b. Institutional framework and entities involved in collection of data and statistics

Lack of mechanisms for systematic monitoring of official statistical data was reported. However, awareness exists of a steady increase in cybersecurity incidents based on the statistics that are produced.

c. Current practices, issues and challenges

Delegates reported that many offences do not result in a complaint or get reported to the authorities, and it can therefore be concluded that there is a high level of unreported offences linked to IT systems.

2.1.3 Tonga

a. Cybercrime Reporting Systems

Tonga has made several improvements in relation to this topic. They now have a greater awareness of the threat of cybercrime, also thanks to the recent establishment of a National CERT. In addition, in 2016 the Cabinet established a Criminal Justice Policy Sub-Committee. This has the remit to implement National Action Plans and Define Criminal Justice Policy. Although the Sub-Committee is currently focusing on violence related criminality as a priority, it has the ability to consider improvements in relation to cybercrimes.

b. Institutional framework and entities involved in collection of data and statistics

Currently the reporting of cybercrimes is almost non-existent, particularly in the public sector. There appears to be no mechanism for front-line police officers to receive complaints and gather the necessary information and evidence to evaluate the need for further investigation. Additionally, there appears to be no formal mechanisms for government departments or the private sector to report cybercrimes or cyber enabled crimes, thus leading to a lack of available statistics.

c. Current practices, issues and challenges

No evidence of current practices for the recording of cybercrimes or cyber enabled crimes.

2.1.4 Morocco

a. Cybercrime Reporting Systems

Morocco has several sources of cybercrime reporting: Police, Gendarmerie, Diplomatic affairs, judicial cooperation and some from bilateral cooperation. There does not appear to be any way of collating these statistics currently, and they are only used for the benefit of the recording agency.

b. Institutional framework and entities involved in collection of data and statistics

Moroccan officials are considering setting up a government reporting system to collect as many reports as possible about the illicit use of digital networks. This government reporting platform will provide reliable statistics on digital offenses in Morocco. Officials would also like to include a team of specialists to analyse the alerts and to take precautionary measures in agreement with the judicial authorities.

c. Current practices, issues and challenges

The Moroccan Ministry of Justice has a system for the compilation of statistics. The data used come from the criminal chain. Unfortunately, this criminal chain does not include all the nomenclature associated with cybercrime offenses. This situation does not make it possible to have currently reliable statistics in the field of cybercrime.

Morocco is looking to:

- Develop a nomenclature for cyber-related/digital offences, which is essential for establishing reliable statistics;
- Expand the program for the integration of statistical tools at all public prosecutors' offices.

2.1.5 Philippines

a. Cybercrime Reporting Systems

On 27 February 2013 the Philippine National Police (PNP) launched the Anti Cybercrime Group with the official acronym "PNP ACG", a National Operational Support Unit primarily responsible for the implementation of pertinent Philippine laws on cybercrime and advocating for the anti-cybercrime campaign of the PNP. A presentation was delivered by Senior Superintendent of the group, who shared cybercrime and electronic evidence statistics, trends and case studies, recorded since the inception of the PNP ACG. The group has a MOU in place with Microsoft Philippines, which is intended to provide training and other programmes to the PNP ACG. From this presentation it was clear that the Group are cooperating with international bodies, i.e. INTERPOL, and proactively investigating cybercrime. However, there was no clarity on other sources of statistics in the country.

b. Institutional framework and entities involved in collection of data and statistics

At present the DOJ-OOC, PNP ACG and NBI-CCD have separate mechanisms for recording reported crime and management of cases under investigation. Collection of criminal justice statistics from the courts is via three sources:

- Supreme Court of the Philippines;
- Court of Appeal;
- Regional Trial Court.

c. Current practices, issues and challenges

Criminal justice statistics for the Philippines are presently not comprehensive. However, they are working toward a single National Justice Information System (NJIS), and work on its creation has begun. The NJIS will provide a single repository for all statistics and is expected to be completed in 2020.

2.1.6 Senegal

a. Cybercrime Reporting Systems

The Dakar Public Prosecutor's Office has a data collection system integrated into the criminal justice system, but there are no facilities for recording cybercrime cases. As a result, there are no reliable cybercrime statistics currently available.

b. Institutional framework and entities involved in collection of data and statistics

The Dakar Prosecutor aims to establish a classification system for cybercrime and cyber enabled crimes.

c. Current practices, issues and challenges

Staff training on classification methods and the use of statistical data is desired and will hopefully be achieved once the idea is validated by the Dakar Prosecutor's Office. This system will be expanded to all the Public Prosecutor's Offices.

2.1.7 Sri Lanka

a. Cybercrime Reporting Systems

Sri Lanka CERT-CC was established in 2006 to protect the country's information infrastructure and

coordinate protective measures against cyber security. It has been the primary cybercrime-reporting centre since that time. CERT-CC receives a variety of its cybercrime reports through its website and over the telephone.

b. Institutional framework and entities involved in collection of data and statistics

Two separate bodies undertake current cybercrime reporting processes in Sri Lanka: one is the National Police, and the other is CERT-CC. The CERT-CC have been the leading agency in the reporting and investigation of cybercrime for many years, and since 2014 the Sri Lanka Police Cyber Crime Unit have begun reporting and investigating such matters.

Both agencies classify the crime reports that they receive in different ways, and whilst they both indicate that they prevent double reporting, there remains some doubt as to whether these figures represent the fullest picture of cybercrime, crimes that are enabled by technology and crimes in which electronic evidence can be utilised in a prosecution.

c. Current practices, issues and challenges

The Sri Lanka CERT reported that although they do keep statistics of incidents reported, three of their main issues are incident duplication, defining incident categories and lack of a common standard of reporting with Law Enforcement and others. They believe the way to address this is with the implementation of an Incident Management System, and will be looking for the Council of Europe to assist in this regard.

2.1.8 Mauritius

a. Cybercrime Reporting Systems

The absence of a centralized system to collect figures and statistics on cybercrime cases that are reported, investigated and prosecuted means that the cybercrime situation in Mauritius can be assessed only on a qualitative basis, by combining information coming from different sources.

b. Institutional framework and entities involved in collection of data and statistics

Cybercrime is reported mainly to police stations, however there are many other departments which can take reports of cybercrime – but there is nothing in place to coordinate this data and ensure collaboration between agencies. The National CERT-MU has a remit to improve this position but does not have the full backing of all stakeholders. Although CERT-MU aims to also represent the interface between the public and the private sectors for cybercrime-related issues, one gap that has been remarked refers to the general reluctance of the financial institutes to report incidents to CERT-MU, such as phishing, mainly due to reputational reasons. Banks are instead obliged to report to the Mauritius Central Bank, which is the only entity holding reliable statistics on the extent of financial cybercrime.

c. Current practices, issues and challenges

CERT-MU and the IT Security Unit (ITSU) of the Ministry for Information and Communication Technology (MICT) have set up a function for central repository of cybercrime statistics, collecting data from all relevant entities. As this is a recent function, it may not yet have complete data or house historic data. Given the current situation of cybercrime reporting, there may also be an underlying risk of double reporting.

The ITSU also estimates that an additional 40% of cases go unreported due to lack of exposure, interaction, training and inadequate procedures.

2.2 International best practices

The afternoon was allocated to international best practices, benchmarking and analysis from organisations with directly relevant experiences.

Three comprehensive, in-depth presentations were delivered by one representative of Ghana, the National Crime Agency, United Kingdom and the National High Tech Crime Unit, France.

Best practice models for collection, interpretation, analysis and dissemination of cybercrime statistics were shared with the delegates.

3 Day 2

Day 2 focussed specifically on how each country currently collects, distributes and exploits crime statistics – and cybercrime statistics in particular –, and how to identify good practices and potential areas of improvement.

3.1 Functional aspects of crime and justice statistics

a. Approaches to Crime and Justice Statistics

There are many different approaches to managing and developing crime and justice statistics, and there is significant international expertise and a body of knowledge in this field. However, there is significantly less knowledge and experience in managing cybercrime statistics. Nonetheless, few countries collect specific statistics relating to cybercrime and this is a more recent area of investigation and research.

A brief overview of an approach is to identify agencies currently collecting relevant cybercrime statistics, understand what they represent, develop processes to describe how they are collected, validated and stored, analyse the data and develop evidence-based policies to address the impact of cybercrime on society.

A comprehensive expertise in statistical numeracy, evaluation and critical thinking are essential skills by those responsible for crime and justice statistics.

b. Under-Reported Crimes Skews Statistics

Crimes are not consistently reported to relevant agencies for investigations. Under-reporting of crime can happen for many reasons, including: a belief that they will not be properly investigated, the challenge of proving that a crime has occurred, a mistaken belief that law enforcement cannot effectively respond to cross-border cybercrimes, the reputational damage caused for businesses, etc.

These challenges need to be recognised and specific measures need to be developed to encourage and support reporting and enhance awareness among end users. Underreported crimes need to be identified, and specific support measures need to be adopted and implemented.

c. Developing Statistics for GLACY+ countries

GLACY+ countries have specific challenges in common and individually, which need to be identified and addressed. Sometimes there are unique strengths in these countries that need to be recognised and supported. The specific challenges need to be identified and quantified, and solutions need to be investigated.

It is then advisable to adopt a country-specific approach in the continuation of this thread of activities.

d. Cybercrime Statistical Sources

There are many public and private organisations, both national and international, which have developed specific sector expertise and knowledge in the field of cybercrime. Organisations maintain records relating to their activities, but the information they are able to share is not always structured or sufficiently comprehensive to offer insights to cybercrime trends.

In many cases, combining data from several platforms, subject to upholding adequate data protection safeguards, can offer subtle, relevant, and detailed information for early warnings of cybercrime challenges.

It is important to identify sources of information and statistics and determine protocols for sharing these data in a controlled manner among trusted peers.

e. Relevant Statistical Categories

Collecting raw data relating to cybercrime from a variety of sources is a fundamental ingredient which then needs to be categorized, collated, validated and securely stored in a secure, structured platform. The categories selected will reflect the purposes, aims and objectives for which they are collected in the first place and need to enable future adaptation for novel or unexpected requirements.

Data validation and qualification is an important criterion for information sources, and it is important that the provenance and history of data sources is linked to the data for future verification or failure tracking.

f. Critical Analysis

Once relevant data sources have been identified and data has been properly and validly collected and then categorized and validated, the purpose of the process is to perform complex, varied, dynamic and continuous analysis of this data to identify relevant markers, trends and milestones in addition to disclosing risks and vulnerabilities identifiable by data stream.

g. Visualisation and Reporting

There is a complex array of vested and independent interested parties to the outcome of the analytical process. The results need to be displayed in a relevant, accurate and clearly understood manner which should be adapted to the target audience, the media being used and the objective of the communication.

For example, information can be displayed for further analysis by academics and professionals active in this field of activity or can be displayed for raising awareness among children and special-needs adults. There are different ways of presenting and visualising this information.

h. Evidence Based Policy

One of the fundamental purposes of this structured approach to collecting and exploiting cybercrime statistics is to develop polices to respond to cybercrime that are based on empirical evidence and changes can be independently measured and tracked. This evidence needs widespread support and trust, and it is critical for effective approaches to cybercrime trends.

i. International Best Practices

GLACY+ offers the ability for countries to work together on developing a nationally relevant and effective approach to collating and analysing cybercrime statistics whilst sharing and learning about best practices and mistakes that others have discovered.

Many countries face similar issues in the complex challenges presented by cybercrime which is trans-national in impact and trans-jurisdictional in nature. It is important that international best practices are shared and understood by all stakeholders in this field.

3.2 Partnership focus on cybercrime and e-evidence statistics

Each GLACY+ country representative was requested to provide answers to three focused questions relating to national approaches towards cybercrime and electronic evidence statistics. Here follows a brief analysis of the results.

a. Describe what your agency currently uses cybercrime statistics for.

This question was designed to identify which agencies are currently collecting cybercrime statistics and what level of awareness they have towards the benefits which ensure from structured collection and analysis of statistics.

b. Describe the key benefits of reliable statistics on cybercrime – for you.

Responses to this question will show the level of understanding towards the importance of reliable sources of statistics. It also emphasises the need to have a consistent approach for recording data, the need to validate data collected and for training for those who collect and record clear coherent data. It will also show an awareness of the possible outputs of data analysis and how it can inform colleagues, management and wider stakeholders relating to cybercrime impacts on society.

c. Describe how your agency could generate a wider range of cybercrime statistics?

Response to this question will highlight the situational high-level awareness of other colleagues, departments, agencies and private sector organisations (both for-profit and not-for-profit) as significant stakeholders who have important knowledge and expertise to contribute in the response to national cybercrime challenges. It helps support and stimulate those countries which are already aware of the need for a comprehensive, cross-sectorial approach to public private partnerships.

Some of the answers were discussed during the morning but the remainder were collated for delivery on the final day. The answers are listed in the following table. The common issues identified are described on Day 3.

a) Describe what your agency currently uses cybercrime statistics for?

PROSECUTORS	**JUDICIAL**	**OTHER**	**LAW ENFORCEMENT**
Budgeting considerations	To ascertain the extent of occurrence of crime	Cybercrime statistics are used for investigations into frauds and to put measures in place to prevent fraud	To inform the authorities about cybercrime trends
Allocation of resources	Effectiveness of dealing with cybercrime	To install necessary IT security measures to prevent future occurrences	To enable the unit to develop strategies
Policy Direction	Case flow management	Inform Policy and budget allocation	To inform Policy and decision-making
Identify rate of convictions	Case distribution to judges with cyber expertise	To improve our risk analysis	Produce strategy on how to prevent cybercrime

Reasons for unsuccessful convictions	Judicial training curriculum development	To deploy counter measures for prevention	Assess current threats and prepare for future events
Effectiveness of deterrence	Setting up courts to deal with the problem of cybercrime	Assess awareness Reporting to Law Enforcement Agencies	For public awareness campaigns
Monitoring current trends in cybercrime	Feedback to stakeholders	To focus on priority issues	Measuring impact on law enforcement
To guide government policy	Highlight the capacity of Police in investigation of cybercrime	Produce a guide on tailor-made security awareness for employees	Measuring law enforcement effectiveness
Identify causes of dismissal of cases	Judicial capacity to adjudicate	Assess the scale of the offences	Identify weakness in infrastructure
	Prosecutions capacity to successfully prosecute	Inform legal powers to aid prevention	To effectively secure more resource
	Public awareness to prompt reporting	To monitor trends worldwide	Analysing the percentage of the public who have been affected by cybercrime
	Reliability of legislation to cater for change in criminal activity	To assess needs for training and other intervention amongst Criminal Justice authorities	Is there a particular category of victim who is more susceptible?
		To formulate National Policy to prevent further cybercrimes	Consider informed resolutions
			Measuring performance
			Measure cybercrime occurrences
			To educate the public about cybercrime
			To seek funding support
			Address immediate challenges
			To produce annual reports
			Policy formulation
			Better training
			Check for previous convictions

b) Describe the key benefits of reliable statistics on cybercrime – for you.

PROSECUTORS	JUDICIAL	OTHER	LAW ENFORCEMENT
Sufficient allocation of staff based on actual requirements	Planning	Understanding and preparing for new threats	Aid management decision making
To identify areas requiring training and capacity building requirements	Resourcing	Intelligence gathering	Educate the public
Use stats not only for detection, but also for prevention	Efficient delivery of justice	Public awareness	Compare on effectiveness of law enforcement
Improve prosecution services to victims	Capacity concerns for the courts	Produce more efficient/relevant policies	Reliable stats on status of investigations and outcomes
	Planning of training for judges	To assess the level of capacities of criminal justice authorities	Knowledge of where to concentrate resources
	Recruitment of judges with cybercrime knowledge	Profiling of cyber criminals	
	Inform legislative changes	Legislative improvements	
		Occurrences of insufficient evidence	

c) Describe how your agency could generate a wider range of cybercrime statistics?

PROSECUTORS	JUDICIAL	OTHER	LAW ENFORCEMENT
Statistics could be generated more efficiently through a centralised system by the Prosecution service.	Complete statistics must be recorded by all units that deal with cybercrime reporting (Police, Customs, Gendarmerie, Judges and courts)	Putting in place systems and processes for collecting and processing data	Fully functional case management system
More information is needed on the cases that do not end with a successful prosecution	Having an effective case management system with additional features to cover cybercrime, cyber-enabled crime, cases involving electronic evidence.	Appoint a single point of contact	A central recording body to disseminate stats to all agencies involved in prevention, detection, prosecution and education and others.

By ensuring that all regional offices have a common reporting template	All agencies record the same type of data to enable uniform information	Connect all agencies in the system	A central collection and processing system
		Introduce an effective reporting strategy to capture the relevant statistics and ensure the right information is supplied to the right agency	Multi stakeholder approach public/private
		A SOP that ensures all agencies share their statistics	Harmonizing categories of data to be used for statistics
		A central system of data collection	Case management system for all stakeholders
		A clear definition of what constitutes cybercrime	Pay for dedicated public surveys/polls
		Wider consultation and collaboration with other agencies	

The afternoon was dedicated to CERTs and CSIRTs in order to stimulate a collective discussion on how governmental agencies deal with statistics, their experiences and case studies. Presentations were made by CERT-GH (Ghana), CERT-MU (Mauritius), SL-CERT (Sri Lanka), CERT.to (Tonga).

4 Day 3

The various discussions and interactions of the first two days were brought together into a commonly agreed approach to developing comprehensive, effective, useful cybercrime and justice statistics.

The first session provided rare insights into two specific international approaches from both common law (United Kingdom) and civil law (France) jurisdictions towards challenges, issues and benefits of public private cooperation in the response towards cybercrime.

The presentations specifically focussed on the areas of sharing information relating to crime intelligence and crime statistics between public/state agencies and private/non-profit organisations.

The second session focussed on further discussions on the results of the questions from Day 2 which were shared and debated with all those present.

The resulting analysis of the responses received from the participants was fully in support of the need for 'best practice' models that had been shared and comprehensively described over the two previous days, and illustrated the similarity between the needs of all agencies.

The common responses included:

a. The strength of a Centralised System for collecting statistics

It is broadly accepted that the responsibility to collect and submit statistics requires dedicated resources. These resources could be located in every agency and organisation that is responsible for their collection, but it is more efficient and effective if this role is dedicated to a centralised system.

In all cases, there will be a need to share data in order to perform effective analytics. Again, a centralised system is a more cost effective and efficient strategy.

b. The need for a common reporting methodology with broad stakeholder support

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

c. The effectiveness of uniform statistics with clear definitions

Uniform statistical definitions will initially take significant effort to be created and will define what specific data is collected and who will be responsible to collect this data in a regular and timely manner. The GLACY+ national stakeholders should validate the agreed definitions and guidelines.

d. The importance of a case management system

Larger 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 maintain appropriate secrecy and confidentiality. A statistical management system will be required for the management of data collected for analysis.

e. The benefits of a single point of contact for each country

A Single Point of Contact (SPoC) for the private sector and Law Enforcement is critical to successful exchange of cybercrime related information.

A single point of contact is either an accredited individual or a group of accredited individuals trained to facilitate effective cooperation between public agencies and the private sector, and with relevant international activities.

f. The positive effect of close collaboration both nationally and internationally

Cybercrime is transborder by its very nature. International cooperation is therefore essential also in the field of collection and comparing relevant statistics. Referring to international standards for the categorization of the sources and the classification of the data to be collected is deemed important and dedicated resourcing, including time, personnel and travel budgets, should be considered.

g. The need for a multi-agency approach which supports cooperation and trust

At a national level the Internet is cross-sector, including all state agencies and private sector organisations. Each stakeholder is an important source of valuable information with a unique perspective on Internet crime trends. During the workshop, several participants were able to share examples of positive outcomes whereby goodwill, customised sharing requests, excellent cooperation – including written protocols between the public and private sector – had ultimately manifested in improved awareness and resilience against cybercrime.

h. The fundamental focus on Cyber enabled/Cybercrime clarity

Many countries have complex systems which track crime and justice statistics, but few countries have protocols which collect statistics on cybercrime and electronic evidence. Many old and widely understood crimes are committed using a computer or communications systems, and we consider these crimes to be cyber-enabled crimes.

However, there are crimes, covered by the Budapest Convention on Cybercrime, which are unique to computer systems. These crimes are not always clearly defined or understood in many criminal laws and are often confused or categorized in pervading standard crime statistics so that the unique crime trends associated with cybercrime is often muted.

It is important to clearly enunciate cyber-enabled and cybercrime events, and track the trends associated with these crimes.

i. The effectiveness of Public-Private Partnerships

This GLACY+ project supports and assists greater positive dialogues and partnerships between state agencies and the private sector with a view to jointly identifying means and methods of cooperation in countering internet related crimes. The project acknowledges the valuable inputs from the private sector to countering cybercrime and the need to maintain constructive collaborative frameworks.

The more frequently these stakeholders meet to address issues of mutual interest without compromising their respective legal roles and responsibilities the better the chances of mitigating cybercrime will be.
The private sector needs recurring training to understand the changing legislator landscape whilst prosecutors and law enforcement officers need to understand and identify the means to capitalise on the fast-changing technological services and statistical data available to them. An attempt to regularise, streamline and standardise the information flow between the two sectors will benefit both sectors.

Presently the level of and effectiveness of cooperation between law enforcement and the private sector is often described as variable. In relation to electronic evidence, sometimes the data legally provided to law enforcement investigators and/or public prosecutors by the private sector data holders is unsuitable for use as evidence is incomplete or not presented in a suitable format for the plethora of different jurisdictions in the world. This can lead to serious delays in the investigation and prosecution of cybercrime-related offences, as well as wasting valuable resources from both the public and private sector actors. In the case of non-evidentiary information, there is a need to clear protocols for the bilateral exchange of data relating to cybercrime trends and crime-related intelligence.

The remaining time on Day 3 was allocated to presenting recommendations for an agreed Methodology for Collection and Analysis of Statistics of Cybercrime and Electronic Evidence. This methodology was created by the Council of Europe experts and is based on prior research from information gathering missions, individual country assessments and the knowledge gleaned from the delegates present at this workshop. This is comprehensively described in the next section.

Different levels of development are noticeable in the GLACY+ countries, where best practice elements are anyway discernible from the various initiatives in progress.

A common methodology for developing effective cybercrime and e-evidence statistical processes could help to systematize the assessment of the current situation, make it comparable with international best practices, and define a suitable action plan to implement improvement actions.

5 Methodology for collection and analysis of criminal justice statistics on cybercrime and electronic evidence

5.1 Expected result

The expected result of this stream of activities is to systematize the collection of criminal justice statistics in order to increase the number of crimes that are reported, investigated, prosecuted and adjudicated, so as to address potential issues that could limit an effective and efficient response to all sorts of cybercrime and cyber-related crimes.

5.2 Related work and international best practices

In the UK, the Home Office publishes Home Office Counting Rules (HOCR)[1]. Crimes are recorded by the Police and others to: ensure that victims of crimes receive the service they expect and deserve; prioritise 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 PCCs, Forces and local partners to build 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.

The Association of Chief Police Officers 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 provide a comprehensive overview of challenges of investigating and prosecuting cybercrime[3].

New questions on fraud and computer misuse were added to the Crime Survey for England and Wales (CSEW) 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[4]. 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[5].

In Scotland, statisticians within the Justice Analytical Services Division[6], 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.

---

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

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

[3] http://www.cps.gov.uk/legal/a_to_c/cybercrime/index.html (last accessed on 6 April2017)

[4] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdec2016#what-has-changed-within-this-publication

[5] 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.

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

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 Europe, the European Network and Information Security Agency publishes a *Good Practice Guide on Cooperative Models for Effective Public Private Partnerships*[7]. This guide classifies 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. A separate report on *Electronic Evidence* provides a *Basic Guide for First Responders*[8]. This guide offers guidance for CSIRTs on how to deal with evidence and the evidence gathering process, including the collection of statistically relevant data.

In 2016, ENISA published a good practice guide of using taxonomies in incident prevention and detection[9]. It provides conclusions and recommendations on improvements that can be made on current cyber incident taxonomies.

In Canada, Statistics Canada[10] is responsible to report on the nature and extent of crime and the administration of criminal and civil justice in Canada. These statistics come within the scope of the following five objectives of the justice system: public order, safety, and national security through prevention and intervention; offender accountability, reintegration, and rehabilitation; public trust, confidence, and respect for the justice system; social equality and access to the justice system for all citizens and serving victims' needs.

In the USA, the Department of Justice, Bureau of Justice Statistics[11], established in 1979, collects, analyzes, 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 needed by federal, state, and local policymakers in combating crime and ensuring that justice is both efficient and evenhanded. The FBI Uniform Crime Reporting (UCR) Program[12] was conceived in 1929 to meet the need for reliable uniform crime statistics for the nation. In 1930, the FBI was tasked with collecting, publishing, and archiving the statistics. Data is received from over 18,000 city, university/college, county, state, tribal, and federal law enforcement agencies voluntarily participating in the program. This data is 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 is submitted either through a state UCR Program or directly to the FBI's UCR Program. The national UCR Program plans to have a New UCR System fully operational in 2017. This will provide enhanced data management tools for greater efficiency in data collection, processing and maintenance of crime data; provide automated processes; provide tailored reports on an as-needed basis, and provide a streamlined publication process that will give users quicker access to the data.

The Australian Cybercrime Online Reporting Network (the ACORN)[13] 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

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

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

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

[10] https://www.statcan.gc.ca/eng/start (last accessed on 6 April 2017)

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

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

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

although not all reports can be investigated. However, reports contribute to the national intelligence database, which is a key component of the fight against cybercrime.

The United Nations Office on Drugs and Crime[14] 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 experts and relevant international organizations. The objective is to enhance the comparability of 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 at the national level, very few platforms collect and publish standardized, reliable statistics on cybercrime at the global level.

It is important to be aware of general statistical principles in the production and dissemination of crime and criminal justice data. Collected data needs to be transparent, accurate and consistent. A central National Collection point can support quality control and Interagency cooperation and further support evidence-based policy changes.

5.3 A preliminary model

Four different phases are involved in acquisition and use of cybercrime statistics:

a. *Crimes Reported (Victims)*

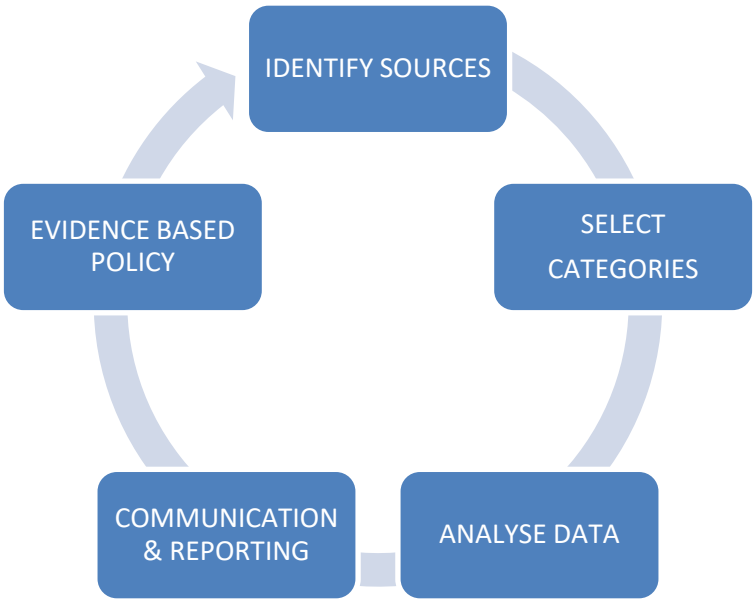
This was the primary focus of the first day, building an overview from information which describes the current reporting systems for each GLACY+ partner, and reviewing this data to identify best practices, gaps, limits and drawbacks.

b. *Crimes Investigated (Law Enforcement)*
Crimes Prosecuted (Prosecution Service)
Crimes Adjudicated (Judiciary)

This was the primary focus of the second day where potential inconsistencies between these numbers were highlighted. An additional focus needs to be dedicated to data relevant to electronic evidence: extracted, analysed, submitted to court, admitted/rejected.

The following preliminary model was presented and adopted during the workshop. It envisages 5 phases:

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



Phase 1. Identify Sources

Identify all the reliable sources of data, according to the local context and according to the rules for crime offences in the local legislation. It is important to identify and involve all the stakeholders and define requirements on the data to be collected. The data should then be collected, possibly in one centralized unit on the national level, and then the characteristics and processes need to be defined (security, data protection issues, confidentiality, etc.). Data validation and consistency is essential.

Phase 2. Select Categories

Develop a method of categorising crimes and data collected so that data duplicates are removed, all reports are included, and data can be easily validated.

Two approaches can be adopted to define categories: by technical description of the different crimes or following the definition of criminal offences in the national criminal code. While the former ensures a more accurate description of the single phenomena that are measured, the latter is preferable as it ensures more stability over the time and, above all, comparability at international level. Then the results from one time period can be compared with another, and so data can be compared between countries.

Phase 3. 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 will also identify errors and gaps.

Phase 4. Communication & Reporting

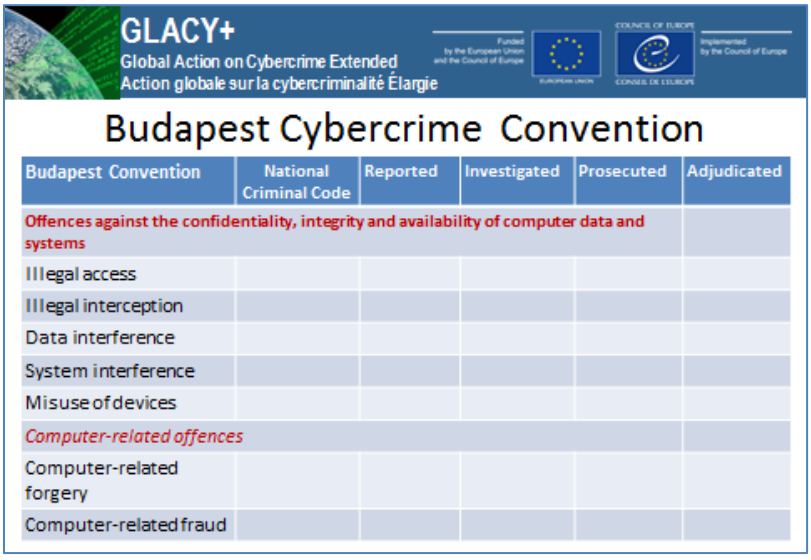
Create aggregated reports on the basis of predefined requirements established by criminal justice authorities, defining the relevant disclosure levels and present data in different ways for different media sources and different target audiences (media, management, politicians, children, etc). Use modern methods of communications.

Phase 5. Evidence Based Policy

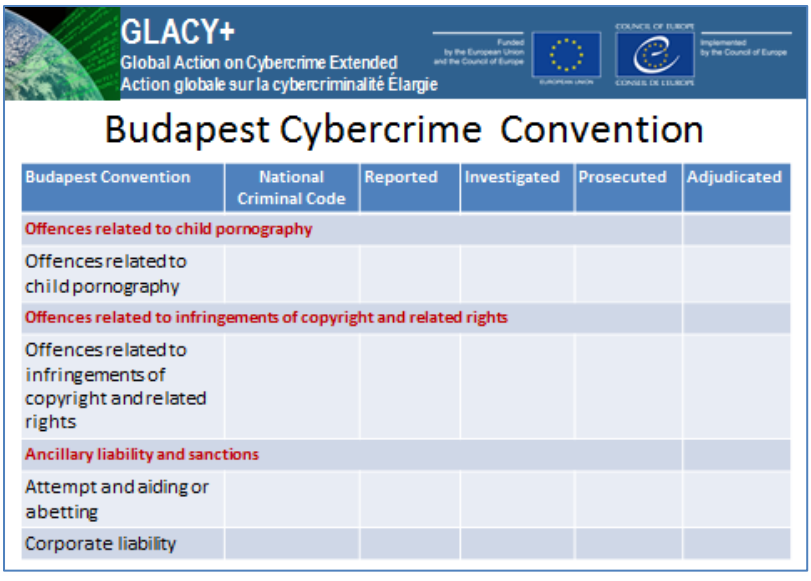
Compare the aims and objectives of published strategies and polices against data collected over longer periods of time to determine levels of effectiveness and possible areas of improvement. Feed the aggregated data back to the policy makers to improve effectiveness of limited resources or gaps in policy or legislation.

In the proposed model, each country should implement in clear written concrete processes with dedicated responsibilities identified at a national level. The model is designed for those responsible for crime and justice statistics at national level.

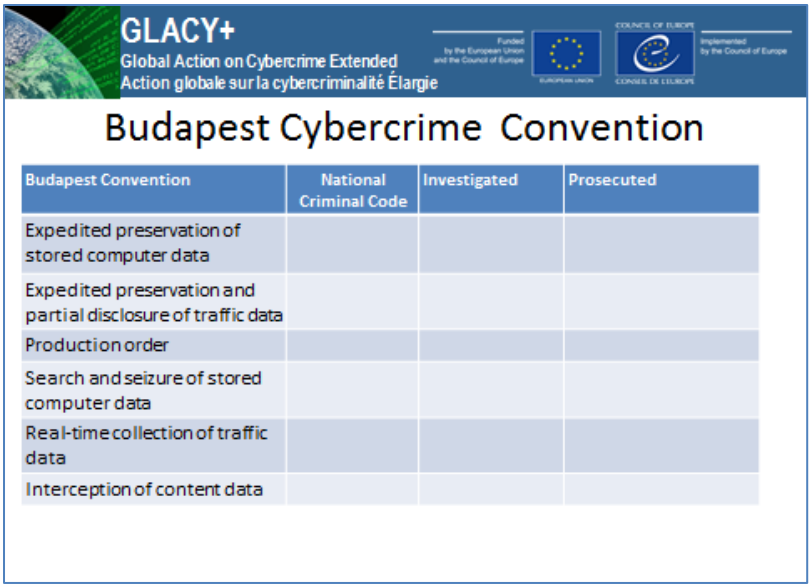
In order to provide an initial starting point for categorising reports, draft template tables could be defined on the basis of the categories of criminal offences foreseen in the Budapest Convention. Each of these offences is usually translated into the national criminal code into locally defined categories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



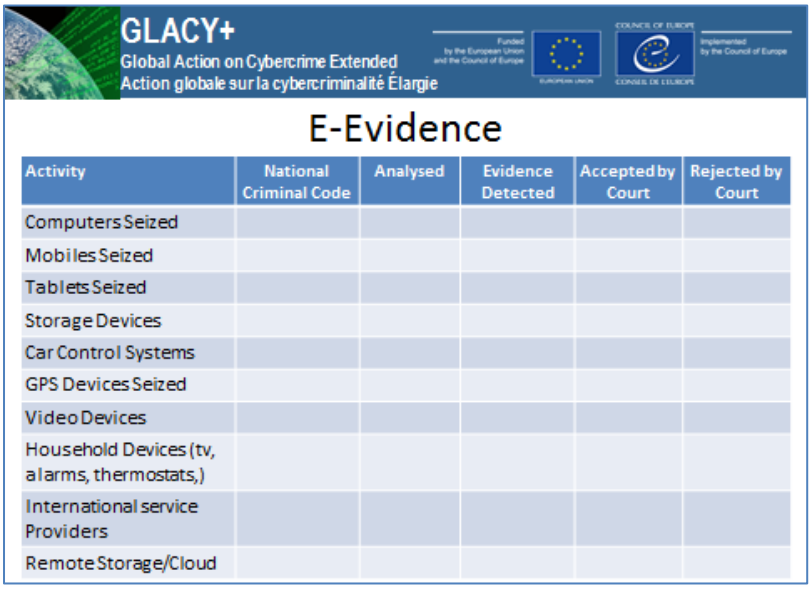
Budapest Convention	National Criminal Code	Reported	Investigated	Prosecuted	Adjudicated
Offences against the confidentiality, integrity and availability of computer data and systems					
Illegal access					
Illegal interception					
Data interference					
System interference					
Misuse of devices					
Computer-related offences					
Computer-related forgery					
Computer-related fraud					



Budapest Convention	National Criminal Code	Reported	Investigated	Prosecuted	Adjudicated
Offences related to child pornography					
Offences related to child pornography					
Offences related to infringements of copyright and related rights					
Offences related to infringements of copyright and related rights					
Ancillary liability and sanctions					
Attempt and aiding or abetting					
Corporate liability					



As far as electronic evidence statistics are concerned, a possible template is provided in the chart below, where reference to the articles of the national legislation could also be given, and the related provisions for Law Enforcement procedural powers.



5.4 Recommendations. Cybercrime and cyber-enabled crimes statistics

A range of specific issues and recommendations were created for each identified phase, to be implemented on a per-country basis during the future individual country visits.

Phase I – Identify Sources:

It would be advisable to implement (or adapt) the **National Cyber Security/ Cybercrime Strategy**:

- To support the creation of a single entity with responsibility for sourcing/collation of Cybercrime statistics (e.g. National Cyber Statistics Office, National CERT, etc.).
    - If single entity is not feasible, to direct multiple entities to source/share 'harmonised' statistics.
- To provide capacities and capabilities by which harmonised statistics are disseminated to all relevant stakeholders, taking into due consideration Data Protection constraints.
- To develop and support public/private partnerships.

Phase II – Select Categories:

- Developing Categories – technical vs. legislation-based approaches.
- Take into account specific challenges of cyber-statistics.
- Need to cover also cyber-enabled crime.
- Need to cover also electronic evidence statistics.
- Adequate training should be provided to first responders, so that proper use of these categories is done when new cases of related crimes are reported/identified.
- Categories can be developed on the basis of the Budapest Convention and how this is translated into National Criminal Code.
- International best practices should be taken into account.

Phase III – Analyse Data:

- Each cybercrime is committed using more than one vector of attack, more than one channel, more than one method. Therefore, the possible presence of redundancies, duplication and improper attribution of crimes to the identified categories should be taken into account.
- Establish method of distinguishing between cybercrime and cyber-enabled crimes.
- Ensure the analysis of any data is conducted by an entity with the necessary skills to create reliable statistics.
- Develop methods of cross reference for verification and for filtering errors.
- Stage1 analysis – identify period, types of crimes, total number of crimes, average number of crimes, crime distribution (region, gender, type of offender, type of victim).
- Stage2 analysis – identify changes since previous analysis including trends, investigate possible bottlenecks.

Phase IV – Communication and Reporting:

- Identify the target whom statistics should be submitted to.
- Display complex data in a manner that encourages understanding and minimises misunderstandings.
- Display data differently for different audiences (colleagues, management, political, public).
- Display data to highlight key messages.
- Display data differently for different channels (web, Facebook, tweets, printed reports, mainstream media, etc.).

Phase V – Evidence-based Policy:

- Identify key messages for decision makers which could have an impact on the legislation/policymaking process.

- Feed aggregated data and statistics to the Cyber Policy cycle, in order for it to be adequately steered on priority areas of intervention.
- Develop and update 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.

5.5 Next steps

Activities will be continued at the national level, relying on the methodological approach given above and on the descending general recommendations. The plan is composed of two further steps:

a. In-country visits to:

- Assess existing procedures for collecting, categorising, analysing, publishing statistics;
- Identify current skillsets available and perform gap analysis;
- Define actionable country-specific recommendations;
- Refine the methodology, tailored for each specific jurisdiction.

b. Develop a country-specific tool kit:

- **Self-assessment models** – develop models for assessing the effectiveness of the system for collecting and analysing cybercrime statistics and e-evidence;
- **Checklists** – to monitor the processes in place and ensure consistency;
- **Template forms** – which could be self-explanatory and require minimum training, prior knowledge or experience;
- **Template agreements** (e.g. MoU) – for interagency cooperation and public–private partnership on exchange of cybercrime data for statistical purposes.

The Council of Europe GLACY+ project team will remain available to actively support and encourage these activities with shared experiences, in-country workshops, regional activities and direct access to other countries outside the GLACY+ partners who have similar interests.