GLACY+

Global Action on Cybercrime Extended
Action globale sur la cybercriminalité Élargie

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

Crime & Justice Statistics

Guidance & Methodology

Andrea Bradley
Cormac Callanan

Council of Europe

Results of yesterday's exercise

Question 1

Describe what your agency currently uses cybercrime statistics for?

Prosecutors

- Budgeting considerations
- Allocation of resources
- Policy Direction
- Identify rate of Convictions
- Reasons for unsuccessful convictions
- Effectiveness of deterrence
- Monitoring current trends in cybercrime
- To guide government policy

Judicial

- To ascertain the extent of occurrence of crime
- Effectiveness of dealing with cybercrime
- Case flow management
- Case distribution to Judges with Cyber expertise
- Judicial training curriculum development
- Setting up courts to deal with the problem of cybercrime
- Feedback to stakeholders

Other Departments

- To focus on priority issues
- Produce a guide in tailor-made security awareness for employees
- Inform legal powers to aid prevention
- To assess needs for training and other intervention amongst Criminal Justice authorities
- To formulate National Policy to prevent further cybercrimes

Law Enforcement

- To inform the Authorities about cybercrime trends
- To enable the unit to develop strategies
- To inform Policy and decision making
- Produce strategy on how to prevent cybercrime
- Assess current threats and prepare for future events

Law Enforcement

- Identify weakness in infrastructure
- To effectively secure more resource
- Analysing the percentage of the public who have been affected by cybercrime
- Is there a particular category of victim who is more susceptible?

Question 2 -

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

Prosecutors

- Sufficient allocation of staff based on actual requirements
- To identify areas requiring training and capacity building requirements
- Use stats not only for detection but for prevention
- Improve prosecution services to victims

Judicial

- Planning
- Resourcing
- Efficient delivery of justice
- Capacity concerns for the courts
- Planning of training for judges
- Recruitment of judges with cybercrime knowledge
- Inform legislative changes

Other

- Intelligence gathering
- public awareness
- produce more efficient/relevant policies
- to assess the level of capacities of criminal justice authorities
- Profiling of cyber criminals
- Legislative improvements
- Occurrences of insufficient evidence

Law Enforcement

- Aid management decision making
- Educate the public
- Gauge effectiveness of law enforcement
- Reliable stats on status of investigations and outcomes
- Knowledge of where to concentrate resources

Question 3

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

Prosecutors

- Statistics could be generated more efficiently through a centralised system by the Prosecution service.
- More information is needed on the cases that do not end with a successful prosecution
- By ensuring that all regional offices have a common reporting template

Judicial

- Uniform statistics must be recorded by all units that deal with cybercrime reporting (Police, Customs, Gendarmerie, Judges and courts)
- Having an effective case management system with additional features to cover cybercrime, cyber enabled crime cases involving electronic evidence.
- All agencies record the same type of data to enable uniform information

Other

- Appoint a single point of contact
- Connect all agencies in the system
- Introduce an effective reporting strategy to capture the relevant statistics and ensure the right information is supplied to the right agency
- A SOP that ensures all agencies share their statistics
- A central system of data collection
- A clear definition of what constitutes cybercrime
- Wider consultation and collaboration with other agencies

Law Enforcement

- Fully functional case management system
- A central recording body to disseminate stats to all agencies involved in prevention, detection, prosecution and education and others.
- A central collection and processing system
- Multi stakeholder approach public/private
- Harmonizing categories of data to be used for statistics
- Case management system for all stakeholders
- Pay for dedicated public surveys/polls

Recurring theme…

- centralised system
- common reporting
- Uniform statistics
- case management system
- single point of contact
- collaboration
- multi agency
- Cyber enabled/Cybercrime clarity

Purpose of Statistical Methodology

to systematize the collection of criminal justice statistics

in order to increase the numbers 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.

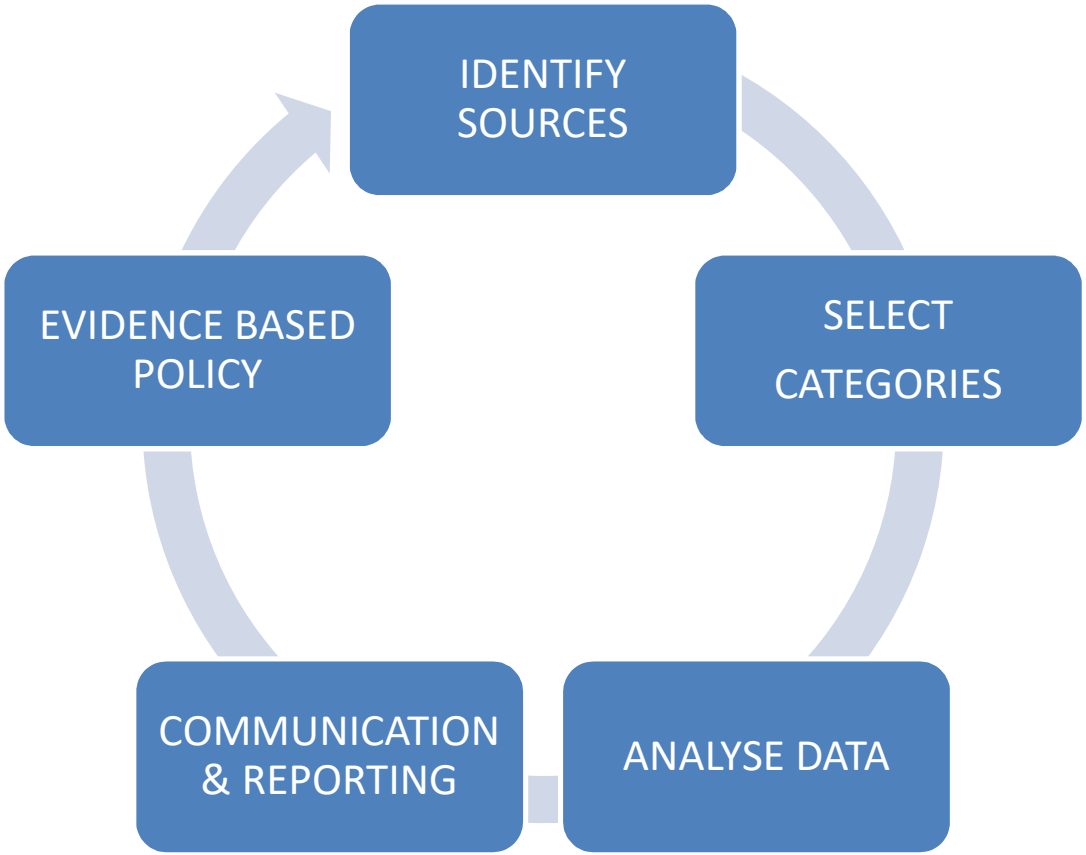
Statistical Methodologies

- Important to be aware of general statistical principles in the production and dissemination of crime and criminal justice data
  - Transparency, Accuracy, Consistency
  - A central national collection point can support quality control and inter-agency coordination
  - for evidence-based policy making
- Supplemental crime victimization surveys are useful

Additional Reasons

- Enhance the comparability of statistics
  - at national level
  - at international level
- Support countries in their efforts to produce national statistics on crime and criminal justice.

Crime Statistics Process



SOURCES

Primary Sources

- Police Crime Statistics
- Prosecutions Services
- Customs
- Court Services
- FIU, Banks
- CERT
- Public-Private Information Sharing
  - ACORN, PHAROS, INHOPE, etc

Supplemental Sources

- Victims Survey
- Public Surveys on Crime Perception
- Others – please suggest
- Public -Proactive detection

Glacy+ Primary Sources

Dominican Republic

Ghana

Mauritius

Morocco

Philippines

Senegal

Sri Lanka

Tonga

Glacy+ Supplemental Sources

Dominican Republic

Ghana

Mauritius

Morocco

Philippines

Senegal

Sri Lanka

Tonga

Recommendations

The implementation (or adaptation) of a **National Cyber Strategy** to:

- Support the creation of a single entity with responsibility for sourcing/collation of Cybercrime statistics. (National Cyber Statistics Office?, CERT?)
- If single entity is not feasible - to direct multiple entities to source/share 'harmonised' statistics.

- To provide the ability to, and the process by which, harmonised statistics are disseminated to all relevant stakeholders. (Data Protection constraints).

- Develop and support public/private partnerships

Taxonomy - Classification

STATISTICAL CATEGORIES

Recommendations.....

- Developing Categories - Criminal/Technical?
- Specific Challenges of Cyber-statistics
- Need to cover cyber-enabled crime
- Need to cover e-evidence activities
- Training for first responders
- Need to account for low conviction rates
- Based on Budapest convention and National Criminal Code
- Consider International best practice

Cybercrime Category List

- Identify Categories
- Crime Codes
- Source Agency (FIU, LEA, CERT, PPP, Banks)
- Include cyber-enabled crime
- E-evidence
- Identify Victims
- Identify Perpetrators

Cybercrime Category List

- Mutually Exclusivity is not possible for cybercrime –
  - committed using more than one vector of attack, more than one channel, more than one method
  - is ascribable to more than one "category" of crime
- Complete/Exhaustive
- Easily Understandable
- Repeatable
- Unambiguous

2014 Donalds C. & Osei-Bryson, K-M "A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction"

Categories – Interesting reading

- Information Architecture
  - Metadata? Thesauri? Taxonomies? Topic Maps! Making sense of it all
- ENISA - Dec2016 - A good practice guide of using taxonomies in incident prevention and detection

Discussion & Feedback

POSSIBLE TABLES

Budapest Cybercrime Convention

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 Cybercrime Convention

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					

Budapest Cybercrime Convention

Budapest Convention	National Criminal Code	Investigated	Prosecuted
Expedited preservation of stored computer data			
Expedited preservation and partial disclosure of traffic data			
Production order			
Search and seizure of stored computer data			
Real-time collection of traffic data			
Interception of content data			

Cyber Enabled Crime

Crime	National Criminal Code	Reported	Investigated	Prosecuted	Adjudicated

E-Evidence

Activity	National Criminal Code	Analysed	Evidence Detected	Accepted by Court	Rejected by Court
Computers Seized					
Mobiles Seized					
Tablets Seized					
Storage Devices					
Car Control Systems					
GPS Devices Seized					
Video Devices					
Household Devices (tv, alarms, thermostats,)					
International service Providers					
Remote Storage/Cloud					

ANALYSIS

Analysis

- Each cybercrime is committed using more than one vector of attack, more than one channel, more than one method

=> is assigned to more than one "category" of crime.

- An efficient collection of statistics should take this into account and, in the analysis phase, eliminate possible duplications and redundancies.

Recommendations

- Establish method of distinguishing between Cybercrime and Cyber enabled crime'
- Ensure the analysis of any data is conducted by an entity with the necessary skills to create reliable statistics
- Prevention of duplication of efforts
- Develop methods of cross reference for verification and to filter errors

Recommendations

- Stage1 analysis – identify period, types of crime, total number of crime, 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

Data Analytics

- Significant Changes
- KPI
- Trends
- Predications
- Anomaly Detection
- Cross Referencing
- Quality Assurance
- Verification

PHAROS Experience

- Scams & extortion 47.58%
- Offenses against minors 11.29%
- Discrimination 10.58%
- Lack of legal qualification 7.28%
- Terrorism 6.93%
- Revelation of facts committed outside the Internet 5.76%
- Threats 2.39%
- Illicit Trafficking 2.14%
- Miscellaneous offenses 1.72%
- Unlawful commercial and professional activities 1.58%

- Infringements of automated data processing systems and electronic devices
- Acts of cruelty to animals
  Violations of privacy
- Offenses against the State and the nation
- Violations against persons
- Extremist movements
- Urban Violence
- Trafficking in human beings
- Provocation of suicide
- Economic and financial offenses
- Immigration networks
- Biomedical Ethics

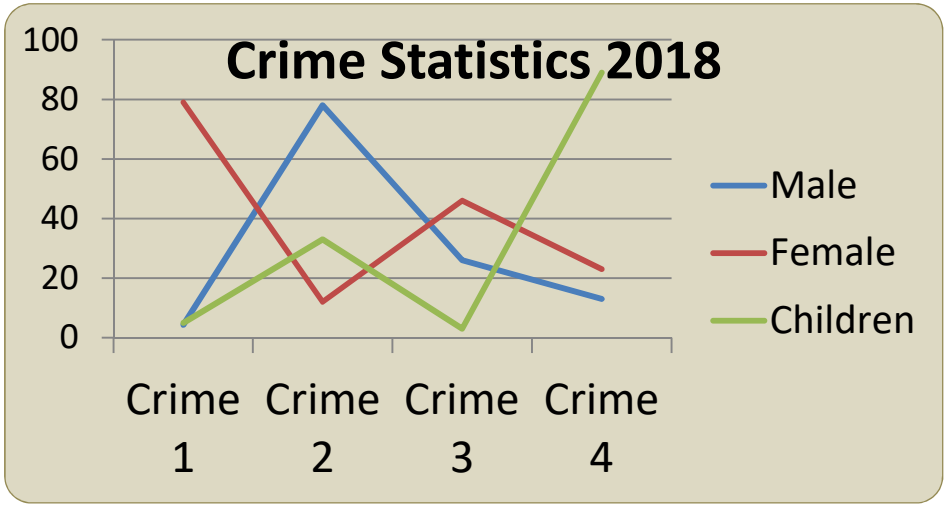
VISUALISATION & REPORTING

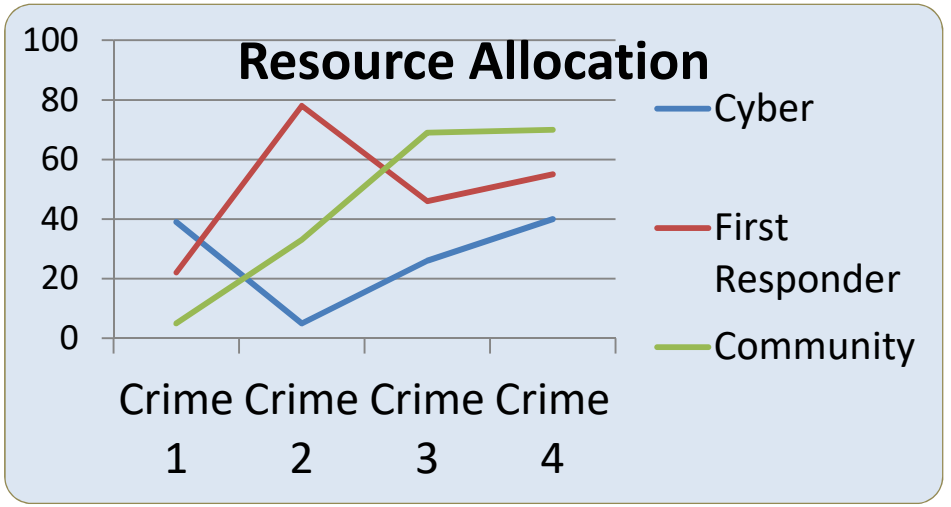
COMMUNICATING

Recommendations

- Display complex data in a manner that encourages understanding
- Minimise mis-understandings
- 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)

- Best to centralise data analysis and visualisation to one location/ organisation





EVIDENCE BASED POLICY

EVIDENCE BASED POLICY

- Strategy Evolution
- Cyber Policies
- Prevention
- Awareness Raising

What next?

In-country visits to:

- Assess existing procedures
- Actionable country specific recommendations
- Refinement of the Methodology

What next?

Create a country specific tool kit:

- Self assessment models
- Checklists
- Template forms
- MoU for interagency cooperation on exchange of cybercrime data for statistical purposes

Continued support with development / implementation.

- Thank you

- Discussion & Debate