Conference “measuring cybercrime in the time of COVID-19:
The role of criminal justice statistics, Strasbourg, 29-30 October 2020

The Budapest Convention and the classification of cybercrime for statistical purposes: some observations

Alexander Seger
Head of Cybercrime Division
Council of Europe
www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

1

Need for data/statistics on cybercrime

- Identify threats and trends
- Inform policy decisions
- Allocate resources
- Transparency, accountability, effectivness and legitimacy of criminal justice action
- Rule of law in cyberspace
- etc.

… in reality very little reporting on cybercrime … does not justify intrusive investigative measures or data retention …

2

Need for data/statistics on cybercrime

- Transparency, accountability, effectivness and **legitimacy** of criminal justice action

Example:

Access to data retained under EU Data Retention Directive (2006)

In 2008: 1.4 million requests for traffic data by LEA in 17 EU m/s but limited information on actual use of such data in criminal proceedings

▶ CJEU 2014: Data Retention Directive invalidated as interference not proportionate

Cybercrime: exaggerated, no data to prove that it is relevant.

3

The concept of cybercrime

Cybercrime?

- Extension of traditional crime but making use of new technologies [excludes conduct that is new in essence]?
- Computer as agent, facilitator or target of crime [too broad]?
- Offences against computers [too narrow?]

Need concept/definition that:

- Covers new and old types of criminal conduct
- But is not too broad to be meaningless
- Is stable even as technology evolves
- Can be operationalised for criminal justice purposes (and statistics)
- Is widely accepted

The Budapest Convention on Cybercrime offers such a concept:

- Offences against computers
- Offences by means of computers but limited to conduct entailing a qualitative change (forgery, fraud, child pornography, IPR)
- Technology neutral
- Used by 100+ countries to criminalise conduct in domestic law (see profiles at **Octopus Community** at **www.coe.int/cybercrime**

4

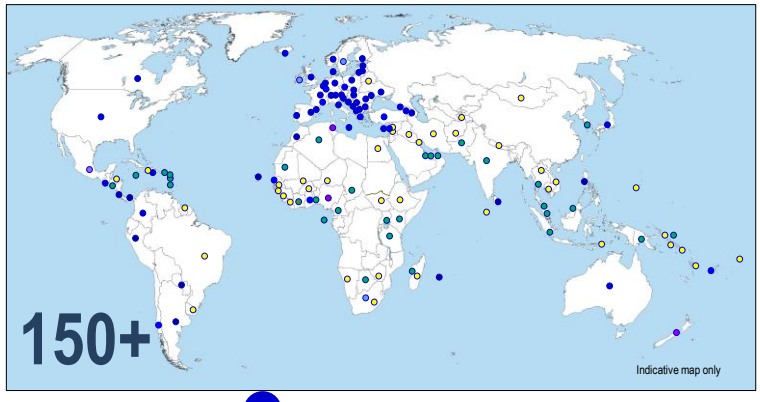
Substantive criminal law provisions of Budapest Convention for classification of cybercrime?

Article	Budapest Convention	Equivalent in domestic criminal law?
Art. 2	Illegal access	
Art. 3	Illegal interception	
Art. 4	Data interference	
Art. 5	System interference	
Art. 6	Misuse of devices	
Art. 7	Computer-related forgery	
Art. 8	Computer-related fraud	
Art. 9	Child pornography	
Art. 10	IPR offences	
Art. 11	Attempt, aiding, abetting	
Art. 12	Corporate liability	

See: Octopus Community at www.coe.int/cybercrime

5

Substantive criminal law provisions of Budapest Convention for classification of cybercrime?



Parties: 65
Signed: 3
Invited to accede: 9
= 77

Other States with laws largely in line with Budapest Convention = 20+
Further States drawing on Budapest Convention for legislation = 50+

6

Substantive criminal law provisions of Budapest Convention for classification of cybercrime?

Substantive criminal (offences against and by means of computer systems corresponding to Articles 2 to 10 Budapest Convention)

See: Octopus Community at www.coe.int/cybercrime

	States	Largely in place by January 2013		Largely in place by February 2020	
All Africa	54	6	11%	22	41%
All Americas	35	10	29%	17	49%
All Asia	42	13	31%	18	43%
All Europe	48	38	79%	44	92%
All Oceania	14	3	21%	5	36%
All	193	70	36%	106	55%

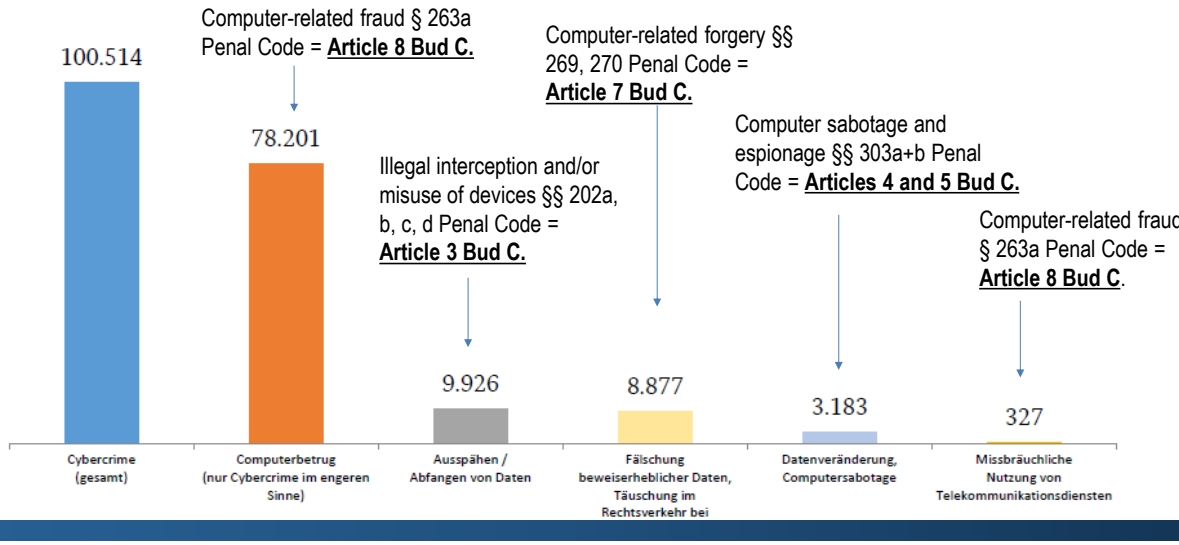
- By February 2020, 106 UN Member States (or 55%) had legislation in place with provisions criminalising offences against and by means of computers similar to those of the Budapest Convention.
- An increase of almost 20% since 2013.

7

Example: German Federal Criminal Police (BKA) – Situation report cybercrime for 2019

(Published September 2020)

Fälle von Cybercrime im engeren Sinne (2019)



8

Example: COVID -19 related cybercrime

COVID-19 related crime in cyberspace

- Phishing campaigns and malware distribution through seemingly genuine information or advice on COVID-19 .
- Ransomware shutting down medical, scientific or other health-related facilities testing for COVID-19 or developing vaccines
- Ransomware targeting individuals through apps claiming to provide genuine information on COVID-19
- Attacks against critical infrastructures or international organizations
- Offenders targeting employees who are teleworking
- Fraud schemes offering personal protective equipment or fake medicines claiming to prevent or cure SARS-CoV-2
- Misinformation or fake news to create panic, social instability, xenophobia, racism or distrust in measures taken health authorities
- Online child sexual exploitation and abuse

Budapest Convention – Articles

- 2 – Illegal access
- 3 – Illegal interception
- 4 – Data interference
- 5 – System interference
- 6 – Misuse of devices
- 7 – Forgery
- 8 – Fraud
- 9 – Child pornography
- 10 – IPR offences

Protocol on Xenophobia and Racism

Guidance Notes on

- Botnets
- DDOS attacks
- Critical information infrastructure attacks
- Malware
- Spam
- ID theft

Procedural powers to secure evidence and identify offenders

- 16+17 – Expedited preservation
- 18 – Production orders
- 19 – Search and seizure
- 20+21 – Interception

With safeguards

- Article 15

Guidance Note on

- Article 18 – Production orders

Framework for international cooperation

- Articles 23 - 35

9

UN ICCS – a framework for criminal justice statistics on cybercrime?

SECTION 09	**ACTS AGAINST PUBLIC SAFETY AND STATE SECURITY**		
0903	**Acts against computer systems** Unauthorized access to, interception of, interference with, or misuse of computer data or computer systems.[128]	+	**Inclusions:** Apply all inclusions listed in 09031 - 09039
		-	**Exclusions:** Possession, distribution or creation of child pornography with a computer system (030221); computer software theft or piracy (0503); possession, distribution or creation of pornography with a computer system (08022); fraud and theft with a computer system (0701) or (0502)
09031	**Unlawful access to a computer system** Unlawful acts involving entry into parts or the whole of a computer system without authorization or justification.[129] - Computer systems as defined in footnote 128.	+	**Inclusions:** Access to a computer system without right; hacking
		-	**Exclusions:** Unlawful access to private computer files that amounts to intrusions upon one's privacy (02011); apply all exclusions listed in 0903
09032	**Unlawful interference with a computer system or computer data** Unlawful acts hindering the functioning of a computer system, as well as acts involving damage, deletion, deterioration, alteration or suppression of computer data without authorization or justification.[130] - Computer systems as defined in footnote 128. - Computer data as defined in footnote 128.	+	**Inclusions:** Damaging, deletion, alteration, suppression of computer data; hindering the functioning of a computer system; denial of service attack, deleting computer system files without authorization; computer system damage; apply all inclusions in 090321 - 090322
		-	**Exclusions:** Damaging property that is not computer data (0504); apply all exclusions listed in 0903
090321	**Unlawful interference with a computer system** Unlawful acts hindering the functioning of a computer system. - Computer systems as defined in footnote 128.	+	**Inclusions:** Hindering the functioning of a computer system; denial of service attack; computer system damage
		-	**Exclusions:** Apply all exclusions listed in 09032

[128] **Computer data**, at minimum, means any representation of facts, information, concepts, in a machine-readable form suitable for processing by a computer/information system. (United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. 2013. Web. <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>).
Computer/information system, at minimum, is a device or interconnected devices which pursuant to a computer/information program perform(s) automatic processing of computer data/information/logical/arithmetic/storage functions including computer data/information stored/ processed/ retrieved/transmitted by the computer/information system including any communication facility or equipment and the Internet. (United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. 2013. Web. <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>).
Computer/information program, at minimum, means instructions in machine readable form that enables a computer/information system to process computer data/information/perform a function/operation and can be executed by a computer/information system. (United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. 2013. Web: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>).
[129] **Access**, at minimum, means to make use of; to gain entry to; to view, display, instruct, or communicate with; to store data in or retrieve data from; to copy, move, add, change, or remove data; or otherwise make use of, configure, or reconfigure any resources of a computer system, or their accessories. (International Telecommunication Union. ITU Toolkit for Cybercrime Legislation. Geneva, Switzerland, 2010. Web: <http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf>).
130 United Nations Office on Drugs and Crime. *Comprehensive Study on Cybercrime*. 2013. Web: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>

85

The UNODC framework on:

"INTERNATIONAL CLASSIFICATION OF CRIME FOR STATISTICAL PURPOSES"

► broadly covers the offences of the Budapest Convention

10

Challenges

0.1% ….. 1%
of cybercrime reported to / recorded by LEA?

bitkom Them

EUR 100 billion damage reported by German industry ⟺ **EUR 82 million recorded by German police**


Pressebereich › Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr

Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr

- 3 von 4 Unternehmen wurden Opfer von Sabotage, Datendiebstahl oder Spionage
- Die Spur zeigt oft nach Osten

Angriffsziel Deutsche Wirtschaft: Drei Viertel sind betroffen

Berlin, 06. November 2019 - Kriminelle Attacken auf Unternehmen verursachen in Deutschland Rekordschäden. Durch Sabotage, Datendiebstahl oder Spionage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 102,9

Nachricht schreiben

Christoph Krösmann
Pressesprecher
E-Mail: c.kroesmann@bitkom.org
Tel.: +49 30 27576-125
Bitkom e.V.


BKA-Lagebild: Computerkriminelle nutzten Corona-Krise für Betrug im großen Stil aus

SICHERHEITSREPORT

FOCUS-Online-Reporter Göran Schattauer

Mittwoch, 30.09.2020, 13:13

Erpressungs-Trojaner, Phishing, Fake-Seiten: Laut BKA wurden 2019 in Deutschland erstmals mehr als 100.000 Cybercrime-Straftaten

11

Challenges

0.1% ….. 1% of cybercrime reported to / recorded by LEA?

WHY?

- Criminal justice too complicated, not efficient, “useless”?
- Attacks against industry and institutions considered matter of national security?
- Self-defence?
- Reputation?
- Insurance pays?
- Unclear legislation and responsilities of LEA (cyberviolence)?
- …..

12

Challenges:

From the 0.1 – 1% of cybercrime that is reported to LEA….

How much is
⇩
Investigated: %?
⇩
Prosecuted: %?
⇩
Adjudicated: 1%?

= 0.001 – 0.01 % of all cybercrime with a conclusive criminal justice response?

= From 100,000 crimes ► 100 – 1,000 reported to / recorded by LEA ► 1 – 10 convictions?

Note: this does not yet include other offences involving electronic evidence.

13

0.01 – 0.001%: What consequences?

- ► Do we have a rule of law problem in cyberspace?
- ► Do governments meet their obligation to protect (K.U. v. Finland)?
- ► Primary government response through cybersecurity, national defence and national security institutions?
- ► Residual response through criminal justice?
- ► Strict rule of law and data protection safeguards for criminal justice v. "margin of appreciation" for national security response?

14

Challenges:

The question of electronic evidence

Budapest Convention

Article 14 – Scope of procedural provisions

1 .....

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c **the collection of evidence in electronic form of a criminal offence.**

Any type of crime may entail electronic evidence:

How to capture that in criminal justice statistics?

15

Challenges

Other challenges:

- Cybercrime often a combination of different offences
- Where cybercrime is a tool to commit more serious offences ► not recorded as cybercrime
- Transnational nature of cybercrime: Offenders, victims, computers, evidence in multiple jurisdictions

Example: TrickBot "takedown" by Microsoft (October 2020):

- What offence/s?
  - Data/system interference
  - Misuse of devices
  - Fraud, forgery
  - Extortion
  - Election interference
  - IPR infringements
  - Etc.
- How many offences, offenders, victims, systems, countries?
  - 2.7 million+ bot infected computers
  - 128 servers

= How to reflect in statistics?

16

Challenges

More challenges:

- Need and relevance of criminal justice statistics on cybercrime and e-evidence recognised but few countries have them
- Few domestic regulations requiring to keep statistics
- No common approach – no comparable data internationally

17

Challenges

Multiple types of data collection and statistics:

- Private sector sources of cybersecurity and -crime data
- CERTs
- Statistics extracted from general databases on crimes recorded (e.g. BKA Lagebericht)
- Platforms for reporting specific forms of cybercrime (e.g. PHAROS/France, Action Fraud/UK) or for cybercrime in general (ACORN (now ReportCyber)/Australia, Internet Crime Complaint Center/USA)

But:

No experience of integrated system of criminal justice data collection on cybercrime reported/recorded, investigated, prosecuted, adjudicated?

[Recommended in EU GENVAL evaluations on cybercrime]

18

Towards a more systematic approach to criminal justice data on cybercrime?

GLACY+ Project: Guide for criminal justice statistics on cybercrime and e-evidence*:

Strategic approach

- Setting objectives: Strategic but SMART
- Environmental scan: structures, institutions, regulations, factors
- Monitoring the plan

Key points for implementation

- Centralised systems to integrate data
- Common reporting methodology
- Uniform definitions of data to be collected
- Case management system
- Clarity in the definition of cybercrime

Steps for data collection

- Identify data sources
- Select categories
- Data analytics
- Communication and reporting
- Evidence-based policy

Data sharing and correlation

- Police, prosecution, courts
- Private sector, CERTs, etc.

Collate and evaluate different types of data/information form multiple sources and draw conclusions?

*Guide by GLACY+/INTERPOL (October 2020).
See also GLACY+ workshop on statistics (Ghana, 2017)

19

Conclusions

Better data / statistics needed to determine:

- Scale, impact, trends of cybercrime
- Effectiveness (and proportionality) of criminal justice response
- Allocation of resources

Common **international** framework for statistics:

- UN ICCS?
- Offences of Budapest Convention

At **domestic** levels:

Promote strategic approach ► Make data collection/statistics part of policies/strategies on cybercrime

- Rules for data collection
- Establish benchmarks for assessing the effectiveness of the criminal justice response
- Use as indicators for allocation of resources to specialised units for cybercrime investigations/computer forensics

COE support through capacity building projects

20