www.coe.int/cybercrime

Mongolia/Council of Europe Cooperation:

Meeting the challenge of cybercrime

alexander.seger@coe.int

Ulaan Baatar, 17 May 2012

1

www.coe.int/cybercrime

Workshop programme:

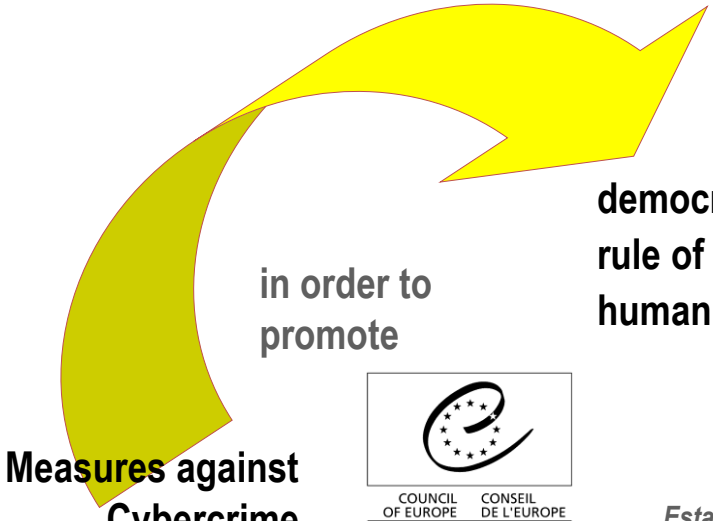
Session 1	Opening
Session 2	What is cybercrime? What strategies?
Session 3	Budapest Convention on Cybercrime
Session 4	Legislation: What offences?
Session 5	Legislation: What tools for investigations? For international cooperation?
Session 6	Institution building and cooperation
Session 7	Lessons learnt during last 10 years?
Closing	Next steps for Mongolia?

Mongolia: Q & Q & Q & Q & Q & A

2

About Council of Europe … www.coe.int

Session 2



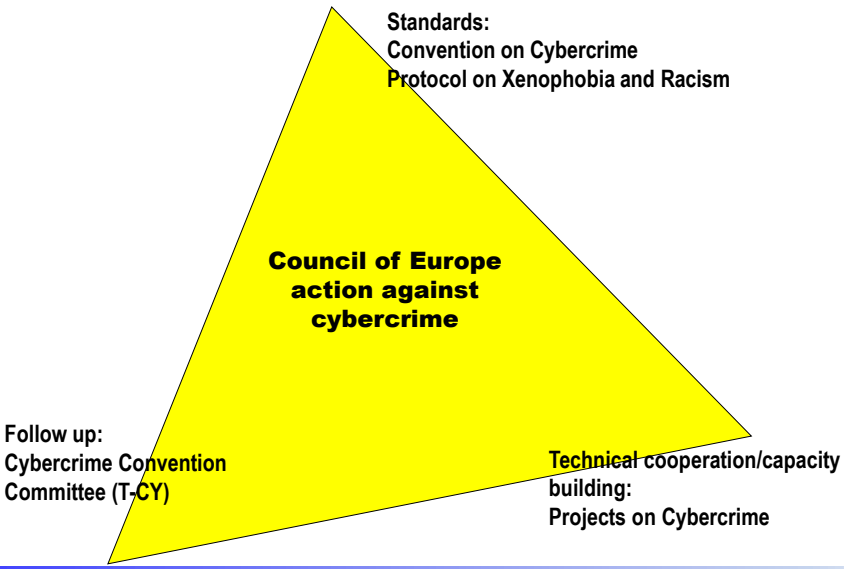
Established in 1949
Currently 47
member States

3

3

Council of Europe approach to cybercrime

Session 2



4

4

About cybercrime

Session 2

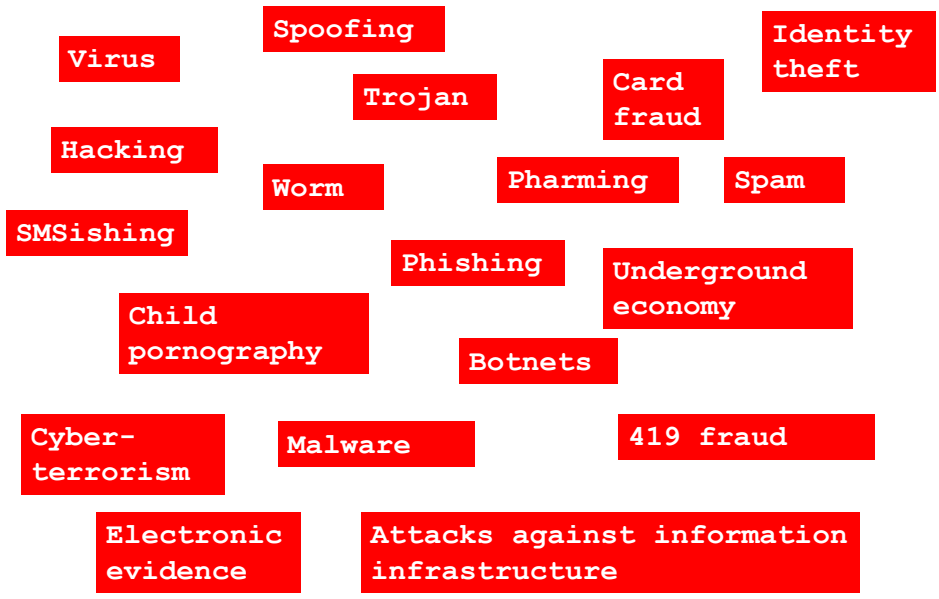
What is cybercrime?

5

5

About cybercrime

Session 2



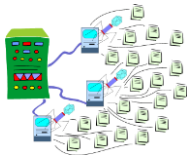
6

6

About cybercrime - tools, infrastructure, platforms

Session 2

- Malware
  - Viruses, worms, trojans ►remove security applications, download additional malware, infect files, steal login and account credentials and other data
  - Web remains main vehicle for malware ►infections by visiting infected sites
  - Email threats ► spam as vector for malware and fraud
- Botnets
  - Main tool for cybercrime and
  - Main risk for cybersecurity (DDOS)
  - Organising for cybercrime



- Criminal domains ►anonymous and „bullet proof“ hosting of criminal domains
- Organising for cybercrime
  - underground economy
  - organised crime
  - persistent threats against political or economic targets
- Money mules
- Technology/context
  - Social networking platforms
  - Cloud computing

About cybercrime

Session 2

How to translate this into a criminal law response?

About cybercrime

Session 2

Offences against the confidentiality, integrity and availability of computer data and systems

- Illegal access (art 2 Budapest Conv.)
- Illegal interception (art 3)
- Data interference (art 4)
- System interference (art 5)
- Misuse of devices (art 6)

Offences by means of computer data and systems

- Forgery and fraud (art 7 + 8)
- Child pornography (art 9)
- IPR-offences (art 10)
- Any other offence (see art 14.2)

Combination of offences:

- Fraud (including identity theft) and other proceeds generating crime
- Attacks against infrastructure
- Organised crime
- Terrorist use of the Interrnet
- Any crime by means of a computer system

▶Electronic evidence

9

9

Cybercrime vs cybersecurity

Session 2

Cybercrime and cybersecurity: what is the difference?

10

10

Cybercrime vs cybersecurity

Session 2

Cybersecurity

Typically defined as:
the protection of the confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT

Motivated by:
- Reliance on ICT -> national interest
- Economic potential of ICT
- CIIP -> National security

Protection against:
- Non-intentional incidents
- Intentional attacks by state and non-state actors against ICT (c-i-a attacks)

Measures:
- Protection, mitigation, recovery through technical, procedural, institutional measures (vulnerability analyses, early warning/response, CERT/CSIRTs, etc)
- Cybercrime legislation, investigation, international cooperation

11

11

Cybercrime vs cybersecurity

Session 2

Cybercrime

Defined as:
- Offences against computer data and systems (c-i-a offences) (Articles 2-6 Budapest Convention)
- Offences by means of computers (such as Articles 7-10 Budapest Convention)

Motivated by:
- Crime prevention and criminal justice

Protection against:
- Intentional attacks against and by means of computers
- Any crime involving electronic evidence on a computer system

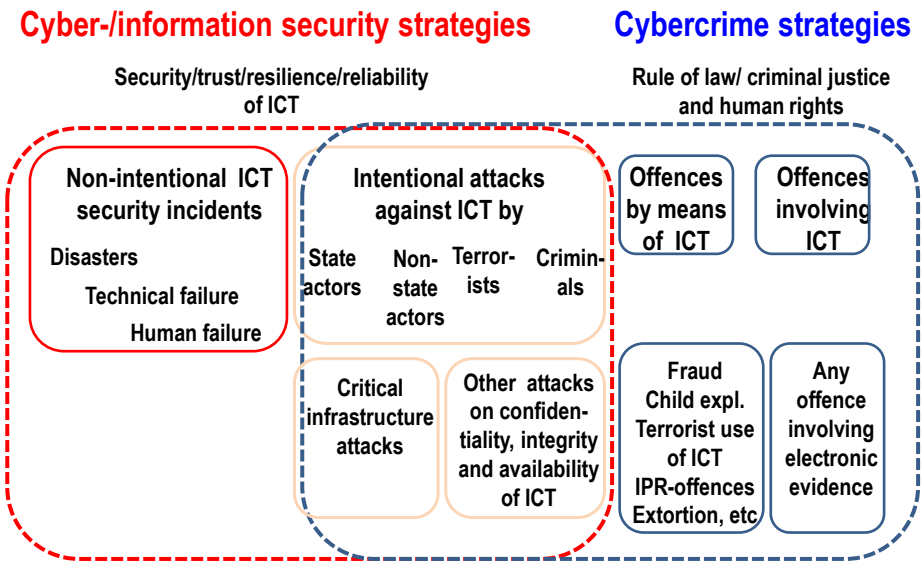
Measures:
- Investigation, prosecution, adjudication
- Conditions and safeguards
- Prevention
- Technical and other measures

12

12

Cybercrime vs cybersecurity

Session 2



13

13

Elements of a cybercrime strategy

Session 2

- Cybercrime reporting
- Prevention
- Legislation, incl. safeguards and data protection
- Specialised units
- Interagency cooperation
- Law enforcement training
- Judicial training
- Public/private cooperation
- Effective international cooperation
- Financial investigations and fraud/ML/TF prevention
- Protection of children

14

14

About the

Budapest Convention on Cybercrime

About Budapest Convention

Opened for signature November 2001 in Budapest

Followed by Cybercrime Convention Committee (T-CY) = Committee of the Parties

As at April 2012:

- **33 parties (32 European and USA)**
- **14 signatories (10 European, Canada, Japan, South Africa)**
- **8 states invited to accede (Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines, Senegal)**

= 55 states are parties/are committed to become parties

- **Many more have used Budapest Convention as a guideline for domestic legislation**

About Budapest Convention

Session 3

Note:

- Guideline + treaty
- Generic (conduct) + specific
- Negotiated + accepted
- Scalable
  - Membership
  - Contents (protools)
  - Link to other standards
- Mature and proven to work:
  - 10 y+ preparation
  - 10 y implementation
- Risk of lower standards and digital divide if new treaty were prepared

17

17

About Budapest Convention on Cybercrime

Session 3

About cybercrime

- Offences against confidentiality, integrity and availability of computer data and systems
- Offenses by means of computers
- Electronic evidence related to any crime
- Volatile evidence
- Transnational crime and evidence
- Technologica change

Legislative response

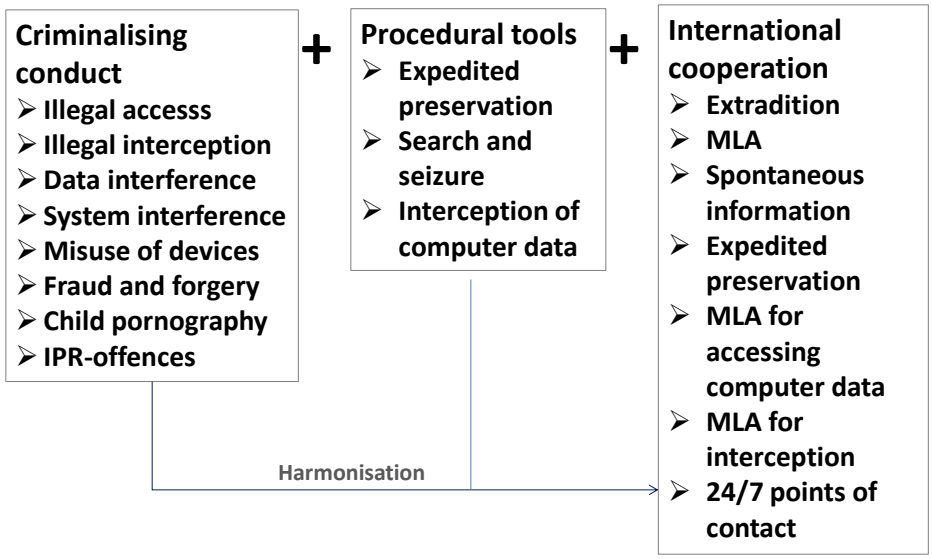
- Criminalise
  - C-i-a offences
  - Offences by means of computers
  - Conduct ≠ technology
- Efficient tools to secure e-evidence related to any crime
- Efficient international cooperation
- International harmonisation of legislation

18

18

Scope of the Budapest Convention on Cybercrime

Session 3



19

19

About Budapest Convention

Session 3

Treaty open for accession (article 37)

Phase 1:
- A country with legislation in place or advanced stage
- Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:
- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession

20

20

Legislation:

What do you need?

What do you have already?

What conduct is a crime?

▶ Substantive criminal law

The legal framework: Substantive criminal law

Session 4

Article	Budapest Convention	Domestic law
Art. 1	Definitions	
Art. 2	Illegal access	
Art. 3	Illegal interception	
Art. 4	Data interference	Art.226 Criminal Code?
Art. 5	System interference	
Art. 6	Misuse of devices	Art. 228 and 229 CC
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	

23

23

The legal framework: Substantive criminal law

Session 4

Article 2 of the Convention: illegal access

Establish as criminal offences under domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system

Article 227 Criminal Code Illegally obtaining of the computer data

227.1. Copying of the data stored in a computer without permission or obtaining it in other ways, as well as actual or attempted interception of the data transmitted through such shall be punishable by …

24

24

The legal framework: Substantive criminal law

Session 4

Article 3 of the Convention: illegal interception

Establish as criminal offences under domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 227 Criminal Code Illegally obtaining of the computer data

227.1. Copying of the data stored in a computer without permission or obtaining it in other ways, as well as actual or attempted interception of the data transmitted through such shall be punishable by …

25

25

The legal framework: Substantive criminal law

Session 4

Article 4 of the Convention: data interference

Establish as criminal offences under domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 of the Convention: system interference

Establish as criminal offences under domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 226 Criminal Code Alteration, damage or destruction of the computer data or software

226.1. Causing a considerable damage by intentional alteration, damage or destruction of the data stored in a computer network or software, rendering its hardware impossible to use or destruction of a data network shall be punishable by …..

26

26

The legal framework: Substantive criminal law

Session 4

Article 6 - Misuse of devices

1 Establish as criminal offences under domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

Article 227. Preparation and sale of devices for illegally entering the computer data Network

Article 229. Designing, using or dissemination of a computer virus

229.1. Designing a computer software with a view of unauthorized deleting, blocking alteration, or copying of the computer data, designing, knowingly using or dissemination of a computer virus shall be punishable

27

27

The legal framework: Substantive criminal law

Session 4

Article	Budapest Convention	Domestic law
Art. 1	Definitions	
Art. 2	Illegal access	
Art. 3	Illegal interception	
Art. 4	Data interference	Art.226 Criminal Code?
Art. 5	System interference	
Art. 6	Misuse of devices	Art. 228 and 229 CC
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	

28

28

The legal framework

Session 4

Offences against the confidentiality, integrity and availability of computer data and systems

- Illegal access (art 2 Budapest Conv.)
- Illegal interception (art 3)
- Data interference (art 4)
- System interference (art 5)
- Misuse of devices (art 6)

Offences by means of computer data and systems

- Forgery and fraud (art 7 + 8)
- Child pornography (art 9)
- IPR-offences (art 10)
- Any other offences (see art 14.2)

Example:

1. Criminals infect legitimate website/malicious adverts (art 4 + 6 + 7)
2. Users accessing sites are redirected to a site from where an exploit kit is downloaded (art 3 + 4)
3. Trojan horse is downloaded to the user`s computer that is now an externally controlled bot (robot, zombie) (art 2 + 5)
4. User accesses bank account online; Trojan transfers login and other credentials to CC server (art 3)
5. Data of bank transaction form is sent to CC server, instead of bank (art 3 + 8)
6. System of CC servers decrypts information and selects a mule account
7. Trojan receives instructions to send an updated transaction form to bank to transfer money to a mule account (art 8)

29

The legal framework: Procedural law

Session 5

What legal powers for investigators and prosecutors:

▶ Procedural criminal law

+ safeguards

30

30

The legal framework: Procedural law

Session 5

Article	Budapest Convention	Domestic law
Art. 15	Conditions and safeguards	
Art. 16	Expedited preservation	
Art. 17	Expedited preservation and partial disclosure of traffic data	
Art. 18	Production order	
Art. 19	Search and seizure	
Art. 20	Real-time collection traffic data	
Art. 21	Interception of content data	
Art. 22	Jurisdiction	

31

The legal framework – procedural law safeguards

Session 5

Procedural powers (articles 16 to 21 Budapest Convention) are to be:

"subject to conditions and safeguards provided for under its domestic law which shall provide for the adequate protection of human rights and liberties..." (article 15)

32

The legal framework – procedural law safeguards Session 5

In general terms, one would expect a State to meet rule of law requirements such as:

- **There shall be no punishment without a law**
- **Everyone has the right to a fair trial, including the presumption of innocence**
- **Interference in the rights of individuals only in accordance with the law and as is necessary in the public interest – including crime prevention – or the protection of the rights of others. Investigative measures are to be prescribed by law**
- **Anyone whose rights are violated must have the right to an effective remedy**
- **States to put in place a framework that allows to reconcile different interests that are to be protected**
- **positive obligation by states to protect the rights of individuals. This may include criminal law and effective enforcement to bring offenders to justice**

33

The legal framework – procedural law safeguards Session 5

- **Principle of proportionality**, meaning in particular that "the power or procedure shall be proportional to the nature and circumstances of the offence". For example, particularly intrusive measures, such as interception, are to be limited to serious offences
- **Judicial or other independent supervision**
- **Grounds justifying the application of the power or procedure and the limitation on the scope or the duration**
- **Powers and procedures must be reasonable and "consider the impact on the rights, responsibilities and legitimate interests of third parties"**

34

The legal framework: International cooperation

Session 5

How to enable efficient international cooperation?

35

35

The legal framework: International cooperation

Session 5

Article	Budapest Convention	Domestic law
Art. 23	General princip. (subsidiarity)	
Art. 24	Extradition	
Art. 25	General rules	
Art. 26	Spontaneous information	
Art. 27	MLA in absence of treaty	
Art. 28	Confidentiality	
Art. 29	Expedited preservation	
Art. 30	Partial disclosure traffic data	
Art. 31	MLA accessing data	
Art. 32	Transborder access	
Art. 33	MLA collection traffic data	
Art. 34	MLA interception content	
Art. 35	24/7 point of contact	

36

36

Once you have the laws: what is next?

- Law enforcement training
- Judicial training
- Specialised institutions
- Law enforcement/service provider cooperation

Institution building and cooperation

Session 6

Law enforcement training strategies - Elements

Justification for adopting/investing in a strategy:

- Reliance on ICT
- Most crime involve e-evidence
- All LEOs to be trained
- Technological developments

Objective of a strategy

To ensure that LEA agencies/officers have the skills/ competencies necessary for their respective functions to

- investigate cybercrime
- secure electronic evidence,
- carry out computer forensics analyses for criminal proceedings
- assist other agencies
- contribute to network security

39

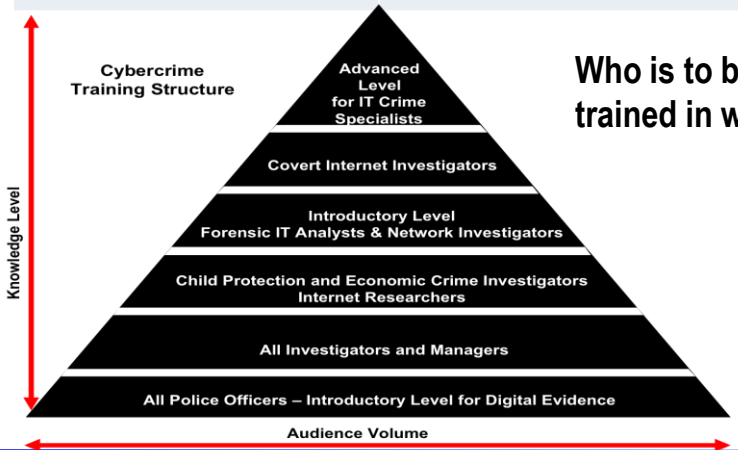
39

Institution building and cooperation

Session 6

Law enforcement training needs analysis

Who	Skills required



Who is to be trained in what?

40

40

Institution building and cooperation

Session 6

Law enforcement training needs programmes

Implementation:

1. Subjects to be trained
2. Training institutions
3. Delivery of training
4. Training materials
5. Updating of materials

41

41

Institution building and cooperation

Session 6

Judicial training concept

Core problem:

- All judges and prosecutors must be prepared to deal with cybercrime
- Existing training too limited and ad hoc, not institutionalised
- Standardised initial and in-service training required
- Need possibility to progress from basic to advanced levels

Purpose of concept 2009:

- to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors
- to integrate such training in regular initial and in-service training

42

42

Institution building and cooperation

Session 6

Judicial training concept

Approach proposed:

1. Institutionalising initial training
2. Institutionalising in-service training
3. Standardised and replicable courses/modules
4. Access to training/self-training materials
5. Pilot centres for basic and advanced training
6. Enhancing knowledge through networking
7. Public private cooperation

43

43

Institution building and cooperation

Session 6

Specialised institutions

Primary role of specialised cybercrime units:

- Investigating and/or prosecuting offences against computer data and systems
- Investigating and/or prosecuting offences committed by means of computer data and systems
- Carrying out computer forensics with respect to electronic evidence in general

Strategic task:

- Cybercrime strategies
- Legislation
- Analysis, intelligence
- Reporting systems, etc.

Tactical tasks:

- Conducting investigations
- Coordination operations
- Collection and analysis of electronic evidence, etc.

44

44

Institution building and cooperation

Session 6

Specialised institutions

Type of specialised units:

- Cybercrime units (crimes against and by means of computers)
- High-tech crime units (crimes against computers)
- Computer forensic units
- Central units (policy, analysis, coordination, support)
- Crime-specific units (e.g. carding, CAM)
- Prosecution-type units

Creating a specialised unit – Steps:

1. Assessing needs and making a decision
2. Legal basis
3. Manager of the unit
4. Staffing the unit
5. Training programme
6. Equipment and other resources
7. Independence of and knowledge about unit
8. Action plan / evaluation mechanism

45

45

Institution building and cooperation

Session 6

Law enforcement/service provider cooperation

Why is such cooperation necessary?

46

46

Institution building and cooperation

Session 6

Law enforcement/service provider cooperation

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime (2008):

- Common measures (including protection of rights and freedoms)
- Measures to be taken by law enforcement
- Measures to be taken by service providers

47

47

Institution building and cooperation

Session 6

Law enforcement/service provider cooperation

Common guidelines for LEA and ISP:

- Develop a culture of cooperation
- Develop written procedures for cooperation with each other
- Cooperate for the protection of rights and freedoms of individuals
- Respect each others roles, rights and limitations
- Mindful of cost of cooperation
- Etc

48

48

Institution building and cooperation

Session 6

Law enforcement/service provider cooperation

Measures to be taken by law enforcement

- Broad and strategic cooperation with ISP
- Procedures for legally binding requests
- Designated and trained personnel for cooperation
- Verification of source of requests
- Standard request format
- Specificity and accuracy of requests
- Follow preservation orders with production/disclosure orders
- Criminal compliance programme

49

49

Institution building and cooperation

Session 6

Law enforcement/service provider cooperation

Measures to be taken by ISPs

- Report criminal incidents
- Assist LEA with training and other support
- Procedures for responding to requests
- Designated and trained personnel for cooperation
- Emergency assistance outside business hours
- Criminal compliance programme
- Verification of source of requests
- Standard response format
- Explanation for information not provided
- Coordination among ISP

50

50

Budapest Convention on Cybercrime 2001 – 2012:

Lessons learnt

Achievements:

- **Process of legislative reforms worldwide**
- **Increased criminal justice measures**
- **Increased trust and cooperation between parties**
- **Global outreach, global impact: 55 countries ratified, signed, invited to accede. Cooperation with at least another 55 countries**
- **Catalyst for capacity building**
- **Increased legal certainty and trust by private sector**
- **An essential element of norms of behaviour for cyberspace**
- **Contribution to human rights and the rule of law in cyberspace**
- **Protection you and your rights**

Cost/benefits of joining Budapest Convention

Benefits

- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Technical assistance and capacity building

"Cost": Commitment to cooperate

Disadvantages: ?

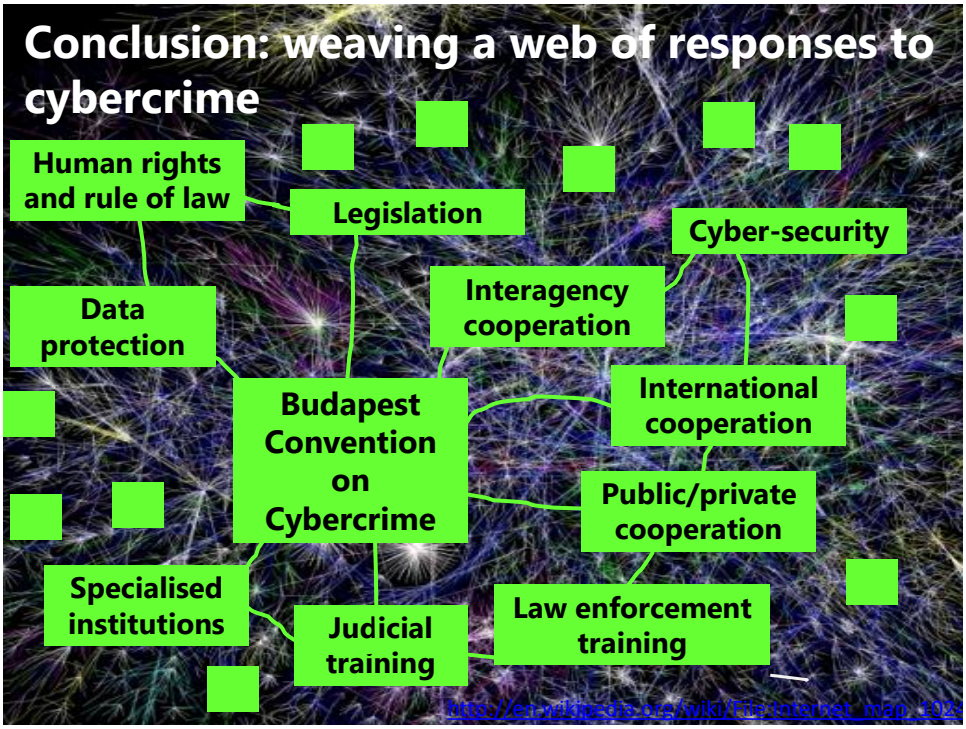
Conclusion: the web is a web

The structure of the Internet

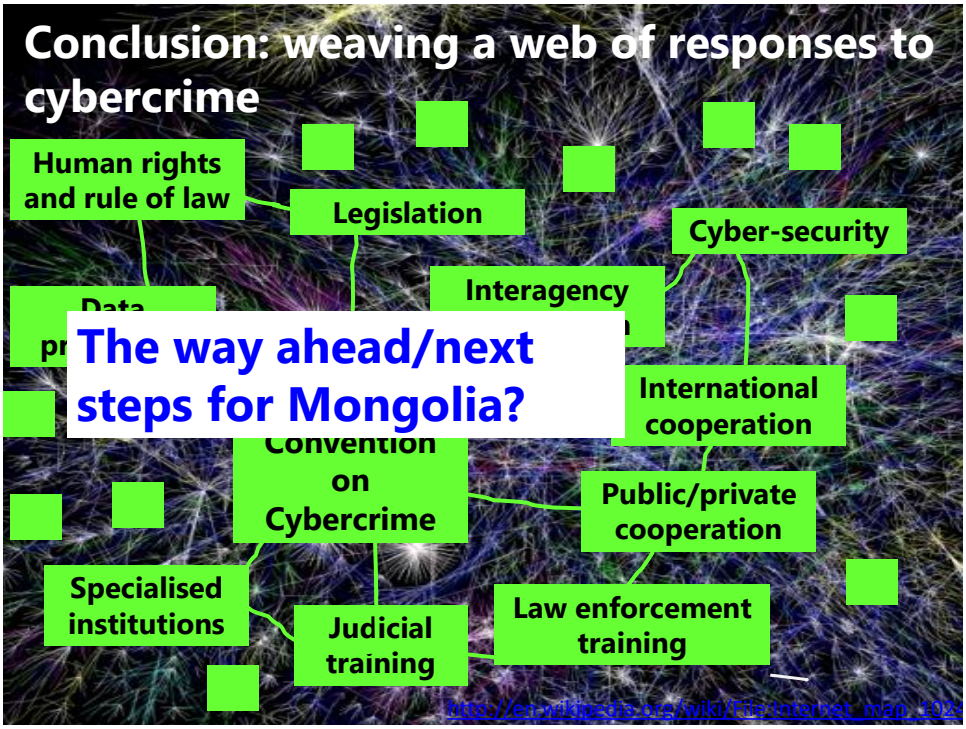
The structure of cybercrime

The structure of the responses to cybercrime

http://en.wikipedia.org/wiki/File:Internet_map_1024.jpg


Conclusion: weaving a web of responses to cybercrime
Human rights and rule of law
Legislation
Cyber-security
Data protection
Interagency cooperation
Budapest Convention on Cybercrime
International cooperation
Public/private cooperation
Specialised institutions
Judicial training
Law enforcement training

55


Conclusion: weaving a web of responses to cybercrime
Human rights and rule of law
Legislation
Cyber-security
Interagency
The way ahead/next steps for Mongolia?
International cooperation
Convention on Cybercrime
Public/private cooperation
Specialised institutions
Judicial training
Law enforcement training

56