Cybercrime, e-evidence and the rule of law in cyberspace:

How relevant is the criminal justice response?

Some hypotheses.

Alexander Seger

Head of Cybercrime Division

Council of Europe

Cybercrime and e-evidence as matters of criminal justice

Hundreds of millions of incidents of theft of personal data every year

Online child sexual abuse

Cyberbullying, harassment and others forms of cyberviolence

Massive fraud generating massive amounts of crime proceeds

Attacks against critical information infrastructure

Ransomware

Interference in computer systems used in elections

+ other offences involving electronic evidence

Threats to

- Human rights
- Democracy
- Rule of law

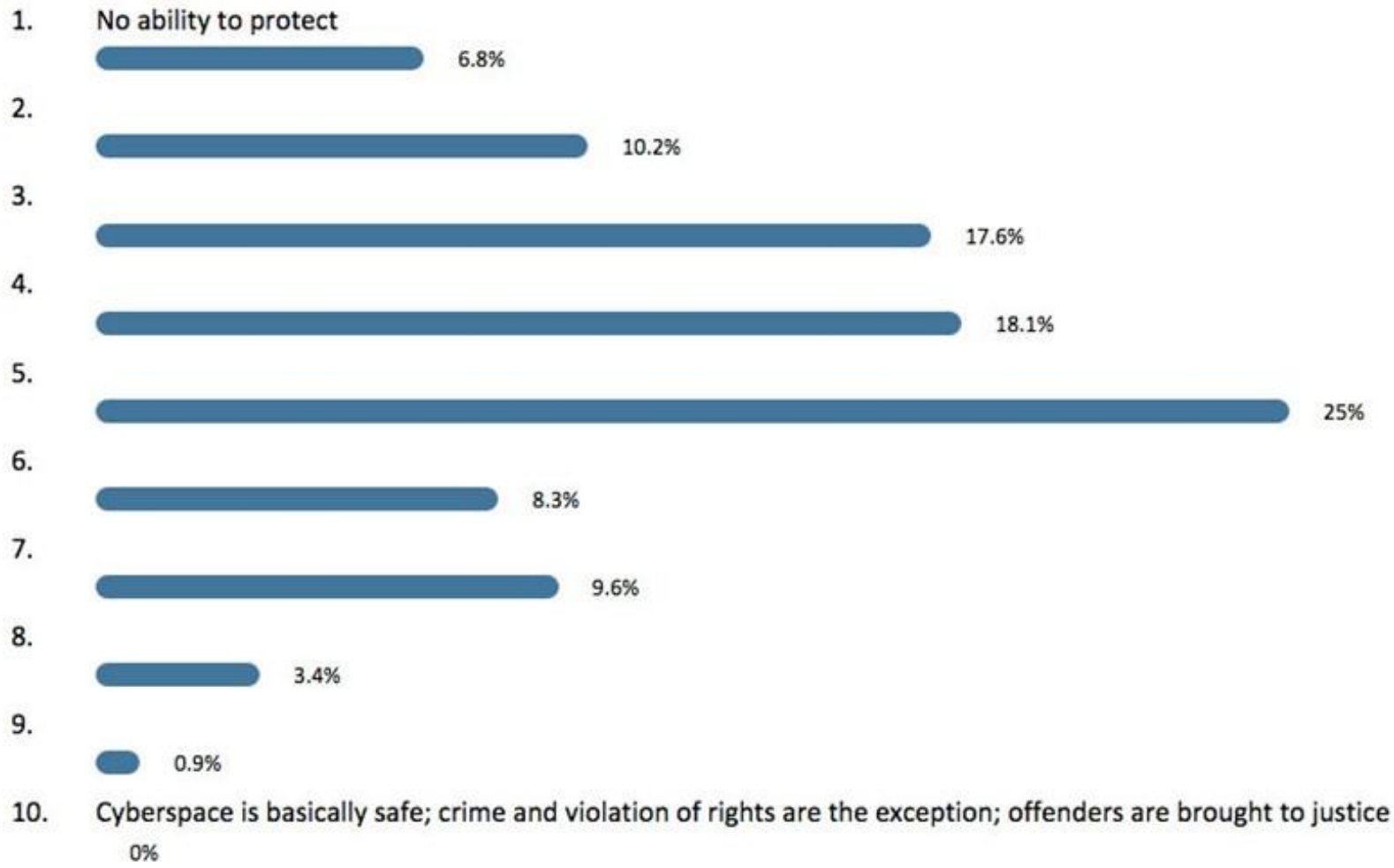
Cybercrime and e-evidence as matters of criminal justice

- Governments have an obligation to protect, including through criminal law (ECtHR 2008: K.U. v Finland)
- Cybercrime and e-evidence require an effective criminal justice response
- Budapest Convention is a criminal justice treaty (specified data in specific investigations)
- Criminal justice response is protective:
  - powers to investigate and prosecute
  - but limited by rule of law conditions and safeguards to protect rights of individuals, including suspects, and prevent abuse

Question: How relevant, how effective is the criminal justice response?

Octopus Conference 2015: Survey among participants

To what extent are governments able to protect individuals/societies against crime and to defend their rights in cyberspace?



Successful investigations on cybercrime globally …

01 Mariposa Botnet Author, Darkcode Crime Forum Admin Arrested in Germany

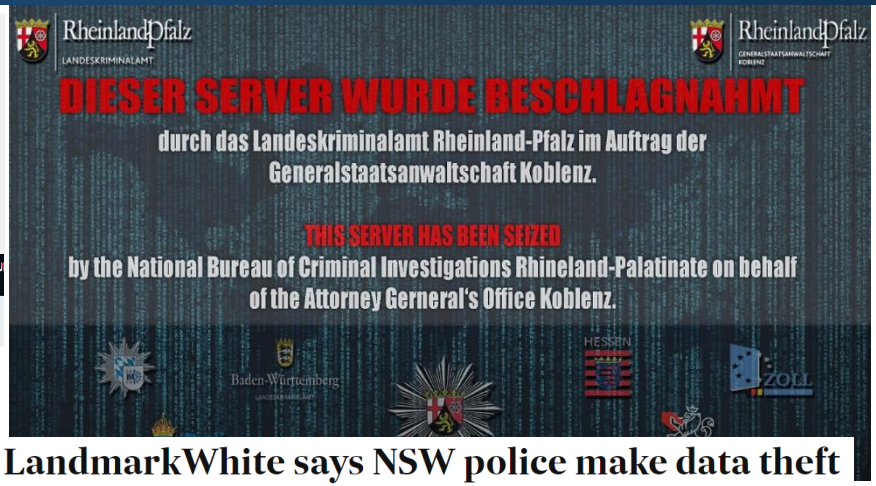
OCT 19

A Slovenian man convicted of authoring the destructive and once-prolific Mariposa botnet and running the infamous Darkode cybercrime forum has been arrested in Germany on request from prosecutors in the United States, who've recently re-indicted him on related charges.

Kerala police arrest 12 for allegedly sharing nude child photos on Whatsapp, Facebook

In a series of raids nicknamed 'Operation P Hunt,' the cybercrime police have also registered 20 cases and seized laptops and mobiles from the arrested.

TNM Staff | Sunday, October 13, 2019 - 13:45



CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA

MUST READ: These 17 iPhone apps have been removed from the Apple App Store for delivering malware

Dutch police take down hornets' nest of DDoS botnets

Police seize servers from bulletproof hosting provider that harbored tens of DDoS botnets

French Cyber Police Take Down Monero Botnet Big Enough "To Bring Down All…Websites on the Planet"

September 1, 2019 @ 9:24 am By Cali Haan

Q1 2019 Hack Blotter: Cybercriminal Investigations, Arrests And Convictions

– Morag McGreevey

Toronto, ON. – Jan. 2, 2019

The last quarter of 2018 saw significant arrests for cyber crime. The biggest news of Q4 is undoubtedly worsening relations between the U.S. and China. In December, the U.S. accused China of a 12-year campaign of cyberattacks targeting technology and trade secrets from corporate computers across almost every global industry. China's Foreign Ministry spokesperson Hua Chunying has denied these allegations, stating that "the Chinese government has never participated in or supported anyone in stealing trade secrets in any way." Read on to see who was investig

LandmarkWhite says NSW police make data theft arrest

Nila Sweeney and Michael Bleby

Oct 2, 2019 — 11.32am

NSW police on Wednesday warned that stolen personal information of Landmark White's clients was still available on the "dark web", despite being removed from the clean, or publicly accessible internet sites.

RELATED QUOTES

LMW $0.17 0.00

601 Chinese arrested for cybercrimes in the Philippines in less than a week

- Manila has launched a crackdown on the large numbers of Chinese who mostly enter the country as tourists and then work for online gambling and cybercrime operations

Fraudsters: EFCC Arrests 280 Cybercrime Suspects In Kano

cording to EFCC, the suspects were arrested for being involved in cybercrimes, money ndering, 'black money', 'wash-wash', 'foxy scheme' and 'MMM'.

BY SAHARAREPORTERS, NEW YORK · SEP 03, 2019

Facebook Twitter Email Share

7,518 views | May 16, 2019, 08:02am

Alleged Cybercrime Kingpin Who Tried To Steal $100 Million From 44,000 PCs Charged

ciated Press

ished: 11:42pm, 17 Sep, 2019

Spanish Police Dismantle Cybercrime Network, Moroccan Police Arrest Suspects

To carry out their fraudulent operations, the cybercriminals sent scam emails to victims asking them to enter their credit card details.

But: What share of cybercrime is reported to and treated by the criminal justice system?

Global cybercrime economy generates over $1.5TN, according to new study

Ground-breaking study, commissioned by Bromium, highlights emergence of Platform Criminality, exposing cybercriminal links to drug production, human trafficking and terrorism

16,144 views | Aug 20, 2019, 06:31am

Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019

One in five women victim of online harassment: report

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

Jacob Knutson Sep 29, 2019

New York Times investigation finds massive spike in online child sex abuse

Last year, tech companies reported over 45 million online photos and videos of children being sexually abused — more than double what they found the previous year.

bitkom

Themen | Marktdaten | Presse | Bitkom

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

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

BKA-BERICHT

Cyberkriminalität in Deutschland nimmt zu – Immer mehr Schadsoftware

Unternehmen und Privatleute werden zunehmend Opfer von Cyberattacken. Die Zahl bösartiger neuer Software steigt laut einem Bericht des Bundeskriminalamtes stark an.

Düsseldorf. Die Zahl der Cyber-Attacken ist im Jahr 2018 um 1,3 Prozent auf rund 87.000 gestiegen, teilte das Bundeskriminalamt (BKA) in seinem Lagebericht zur Cyberkriminalität am Montag mit. Dabei handle es sich allerdings nur um die Angriffe, die der Polizei bekanntgeworden seien. Es entstand ein Schaden von mehr als 60 Millionen Euro.

But: What share of cybercrime is reported to and treated by the criminal justice system?

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)?
- …..

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.

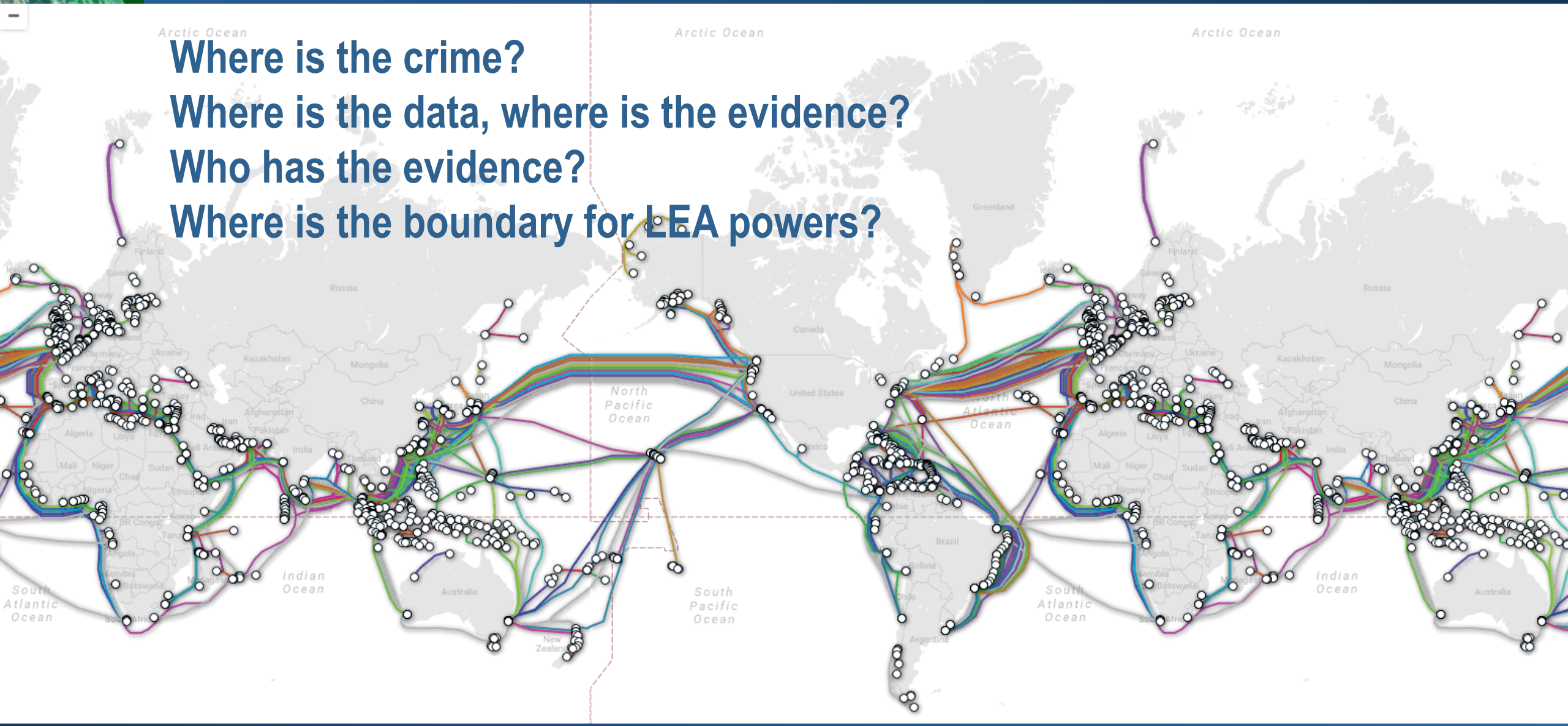
From the 0.1 – 1% of cybercrime that is reported to LEA….

1% Adjudicated

WHY?

Why 1% adjudicated?

Where is the crime?
Where is the data, where is the evidence?
Who has the evidence?
Where is the boundary for LEA powers?



Why 1% adjudicated?

Cybercrime and electronic evidence: challenges for criminal justice:

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, anonymisers, encryption, VOIP, NATs etc.)
- Cloud computing, territoriality and jurisdiction
  - Cloud computing: distributed systems ▶ distributed data ▶ distributed evidence
  - Unclear where data is stored and/or which legal regime applies
  - Service provider under different layers of jurisdiction
  - Unclear which provider for which services controls which data
  - Is data stored or in transit ▶ production orders, search/seizure or interception?
- The challenge of mutual legal assistance
- No data ▶ no evidence ▶ no justice

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?

About safeguards for criminal investigations

Budapest Convention ► criminal law context ► specific investigations ► specified data

Rule of law requirements for investigative measures interfering with rights of individuals:

- must be prescribed by law and the law must meet the requirements of precision, clarity, accessibility and foreseeability;
- must pursue a legitimate aim;
- must be necessary, that is, it must respond to a pressing social need in a democratic society and thus be proportionate;
- must allow for effective remedies;
- must be subject to guarantees against abuse.

Example "direct disclosure":

- Legal basis for specific criminal investigations
- Limited to subscriber information (information needed to identify the subscriber of a service)
- May require to be issued under judicial or other independent supervision
- Information to be provided in the order
- Option of notification requirement with MLA-type grounds for refusal
- Enforcement via "giving effects" or mutual assistance
- Option of reservation on article

+ data protection safeguards (under discussion)

About safeguards for criminal investigations

Data protection safeguards / issues under discussion:

1. General provisions (eg scope, general principles)
2. Purpose and use
3. Onward transfers
4. Quality and integrity of data
5. Information security
6. Data breach notification
7. Maintaining records
8. Retention periods
9. Special categories of data
10. Automated decisions
11. Individual rights / access, rectification, administrative redress, judicial redress
12. Transparency / Notification
13. Oversight / Supervisory authorities

About safeguards for national security measures

Bulk interception of data and mass surveillance for national security purposes ("creating the haystack")

► "Margin of appreciation"?

0.01 – 0.001%: What consequences?

- Further shift of competencies from the ”cumbersome“ criminal justice (with strict safeguards) to the “more efficient” national security arena (with limited safeguards)?
- Limited reliance on criminal justice?
- Limited focus on victims?
- Shift from protecting individuals to protecting critical infrastructure?
- Erosion of trust in public institutions, democracy, and state governed by rule of law and protecting human rights?

How to make the criminal justice response more effective & relevant?

- Dramatic surge in resources and skills for criminal justice authorities, including judiciary
- Multiply capacity building efforts
- Convince decision makers: cybercrime and e-evidence are not marginal issues
- Reform/put in place specific procedural powers (with “proportionate” rule of law conditions and safeguards)
- Provide for additional powers to secure electronic evidence that can effectively be applied in practice ▶ Protocol to Budapest Convention
- Cooperation at all levels and information sharing
- What else? ▶ Use Octopus to come up with solutions!