Cybercrime
Research Institute

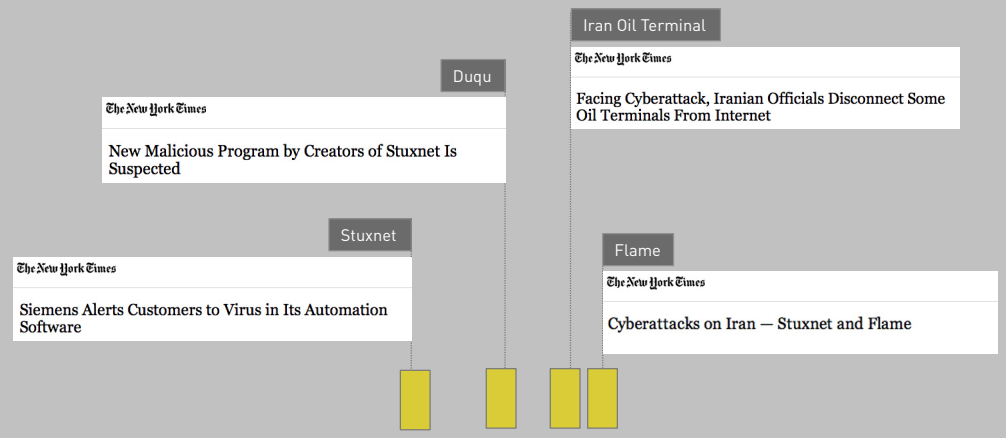
THE NEED FOR NATIONAL LEGISLATION AS WELL AS REGIONAL AND INTERNATIONAL HARMONIZATION IN FIGHTING CYBERCRIME

ESCWA Conference
20.12.2012, Beirut
Prof. Dr. Marco Gercke

Cybercrime
Research Institute

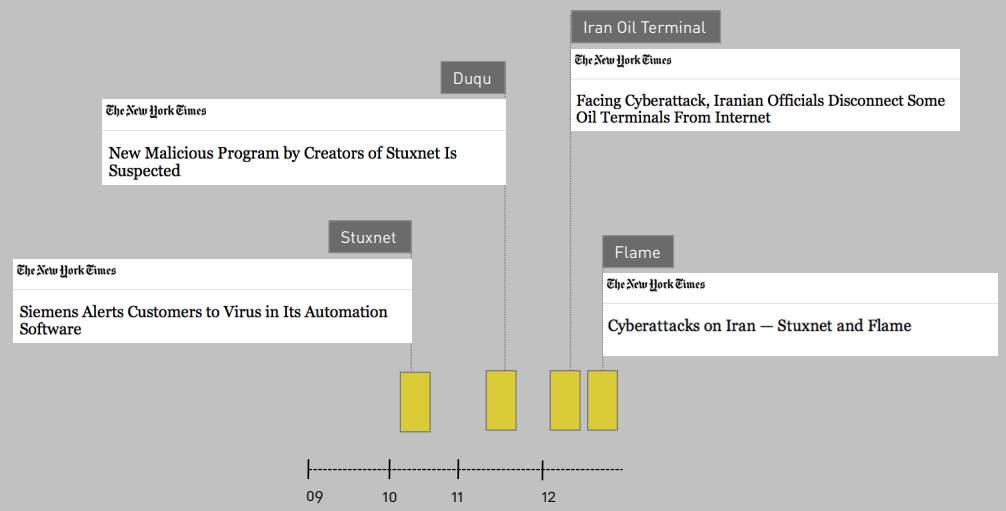
WHY COUNTRIES SHOULD CARE ABOUT CYBER SECURITY AND CRIME

INTRODUCTION

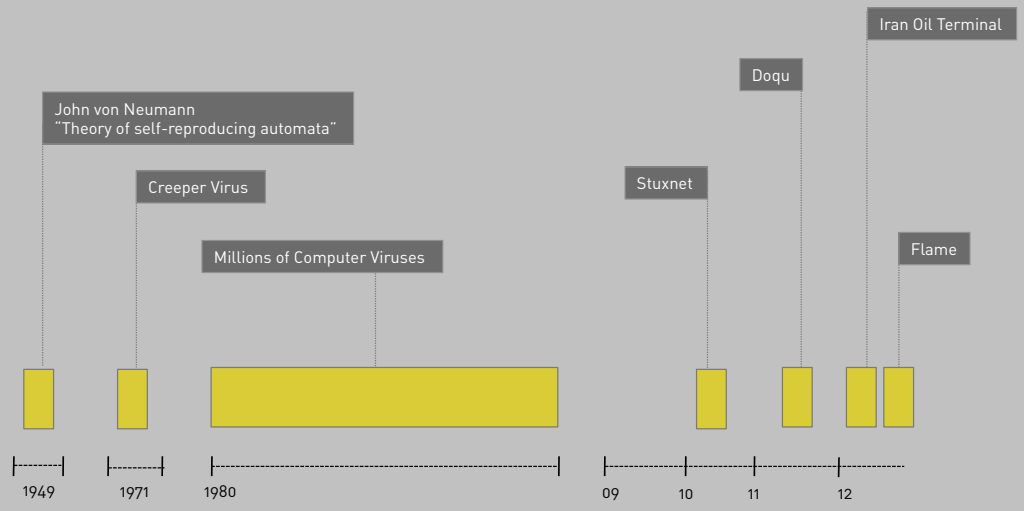


Cybercrime
Research Institute

INTRODUCTION



INTRODUCTION



WHAT HAS CHANGED WITH REGARD TO ATTACKS?

SPY ASPECT

- In the past most spy-related activities required at least once physical presents at the observed location

- Today it is possible to install a spyware remotely on thousands of computer systems in parallel
- Spyware is capable of not only intercepting mail/text communication but also take screenshots, activate microphones and webcams

Picture removed in print version
Bild zur Druckoptimierung entfernt

Estonia

PHYSICAL SABOTAGE

- In the past attacks against nuclear programs where largely carried out against infrastructure

- Stuxnet underlined that the capability of a software tool is not necessary limited to deleting data but it has the potential to physically destroy objects (centrifuges) from the distance without any interference with buildings and life of people.

Picture removed in print version
Bild zur Druckoptimierung entfernt

SYRIA

Cybercrime
Research Institute

WHY SHOULD THERE BE REGIONAL HARMONIZATION?

Cybercrime
Research Institute

COMMONWEALTH OF NATIONS

- The Commonwealth of Nations is a voluntary association of sovereign states
- Currently 53 associated states
- In 2002 the Commonwealth presented a model law on Cybercrime that provides a legal framework to address Cybercrime
- The model law was intentionally drafted in accordance with the Convention on Cybercrime

Picture removed in print version
Bild zur Druckoptimierung entfernt

COMMONWEALTH MEMBER STATES

Cybercrime
Research Institute

COMMONWEALTH OF NATIONS

- In addition to substantive criminal law and procedural law the Commonwealth also discussed the importance of digital evidence
- Without admissibility of digital evidence courts are in most cases unable to sentence offenders
- In 2002 Commonwealth therefore presented a model law on digital evidence

Picture removed in print version
Bild zur Druckoptimierung entfernt

COMMONWEALTH MEMBER STATES

Cybercrime
Research Institute

ECONOMIC COMMUNITY OF WEST AFR.

- The Economic Community of West African States is a regional group of west African Countries
- Founded in 1975 it has currently fifteen member states
- In 2009 ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states
- Directive includes substantive criminal law as well as procedural law

Picture removed in print version
Bild zur Druckoptimierung entfernt

ECOWAS MEMBER STATES

Cybercrime
Research Institute

EAST AFRICAN COMMUNITY

- 5 Member states (Kenya, Uganda, Tanzania, Burundi, Rwanda)
- Within the framework of an update of ICT legislation (EAC Legal Framework for Cyberlaws) EAS also addressed the issues of Cybercrime
- Provisions dealing with the criminalisation of certain conduct became part of the draft legislation

Picture removed in print version
Bild zur Druckoptimierung entfernt

EAC MEMBER STATES

Cybercrime
Research Institute

COMESA

- Common Market of Eastern and Southern Africa
- In 2011 COMESA presented a Cybersecurity model law that included various provisions related to Cybercrime

Picture removed in print version
Bild zur Druckoptimierung entfernt

COMESA

Cybercrime
Research Institute

ESCWA

- United Nations Economic and Social Commission for Western Asia
- Between 2008 – 2011 ESCWA carried out a porject on "regional harmonization of cyber legislation to promote the knowledge society in the Arab world"
- This included the production a harmonization instruments (including Cybercrime

Picture removed in print version
Bild zur Druckoptimierung entfernt
ESCWA

Cybercrime
Research Institute

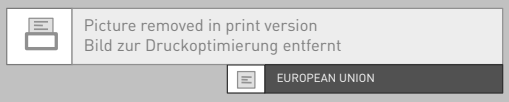
LEAGUE OF ARAB STATES

- In 2003/2004 the Council of Ministers of Justice and the Council of the Ministers of Interior adopted the Emirates Model Arab Law on Combating Information Technology Systems and suchlike Offences

Picture removed in print version
Bild zur Druckoptimierung entfernt
ESCWA

EUROPEAN UNION

- The European Union is a political Union of 27 member states
- One of the mandate of the EU is to harmonise legislation in selected areas
- It has adopted several Framework Decision and Directives to harmonise the legislation with regard to Cybercrime
- The 27 member states are obliged to implement the legislation within the given time period



Cybercrime
Research Institute

Substantive Criminal Law	Illegal Access to a Computer	Illegal Remaining in a Computer	System Interference	Illegal Interception	Illegal Access to Computer- Data	Illegal Data Input	Illegal Aquisition of Comp. Data	Illegal Data Interference	Illegal Use of Data	Violation of Data Protection Regul.	Illegal Devices / Misuse of Devices	Computer-related Fraud	Computer-related Forgery	Indecent Material	Pornography	Child Pornography	Solicitation of Children	Dissemination of Racistic Material	Identity-related Crime	SPAM	Threat and Harassment	Disclosure of an Investigation	Copyright Violation	Violation of Secrecy
Commonwealth Model Law (2002)	✔		✔	✔				✔			✔					✔								
ECOWAS Draft Directive (2009)	✔	✔	✔	✔		✔		✔	✔		✔				✔	✔		✔			✔			
COMESA Model Bill (2011)	✔		✔	✔	✔						✔	✔	✔								✔			
HIPCAR Cybercrime Model Law (2010)	✔	✔	✔	✔			✔	✔			✔	✔	✔			✔	✔		✔	✔	✔	✔		
CoE Cybercrime Convention (2001)	✔		✔	✔				✔			✔	✔	✔			✔							✔	
ICB4PAC Cybercrime Model law (2011)	✔	✔	✔	✔			✔	✔			✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	
Different EU instruments	✔		✔	✔				✔			✔	✔				✔	✔							
Draft African Union Convention (2011)	✔	✔	✔	✔		✔		✔	✔	✔	✔	✔	✔			✔		✔				✔		✔
Commonwealth Model Law (2002)	✔		✔	✔				✔			✔					✔								
HIPCAR Cybercrime Model Law (2010)	✔	✔	✔	✔			✔	✔			✔	✔	✔			✔	✔		✔	✔	✔	✔		
HIPSAA Draft Model	✔	✔	✔	✔			✔	✔			✔	✔	✔		✔	✔		✔	✔	✔	✔	✔		

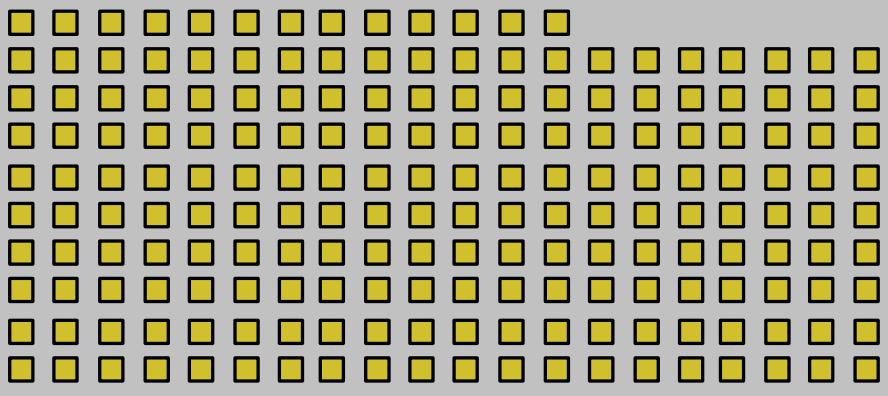
Cybercrime
Research Institute

WHY DO WE NEED INTERNATIONAL HARMONIZATION?

WHY SHOULD ARABIC COUNTRIES BE MORE INVOLVE?

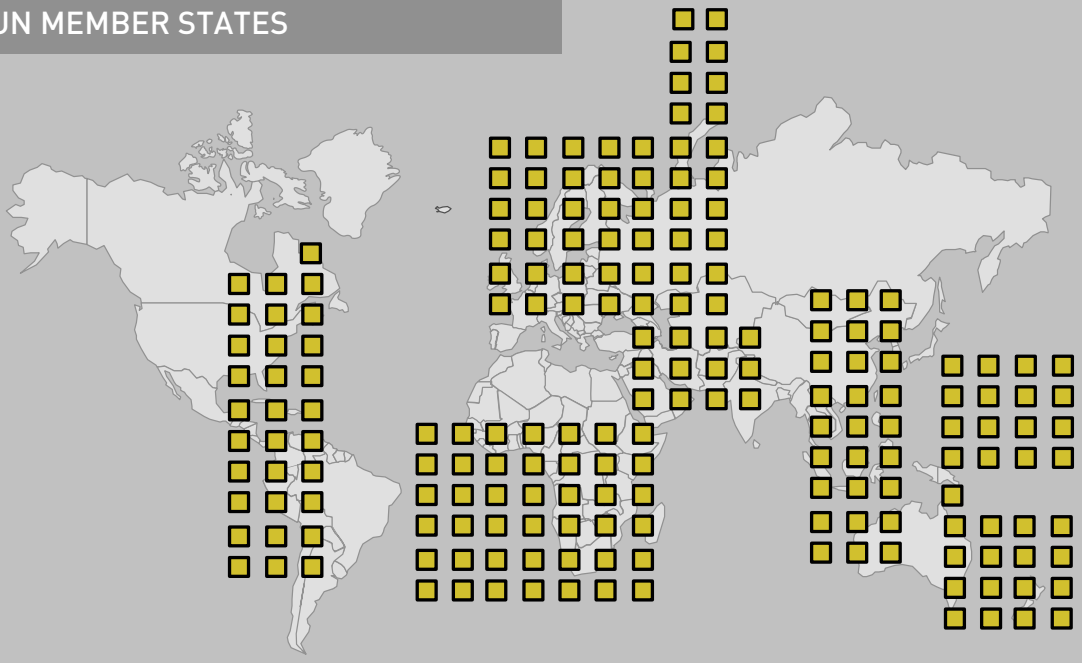
Cybercrime
Research Institute

UN MEMBER STATES



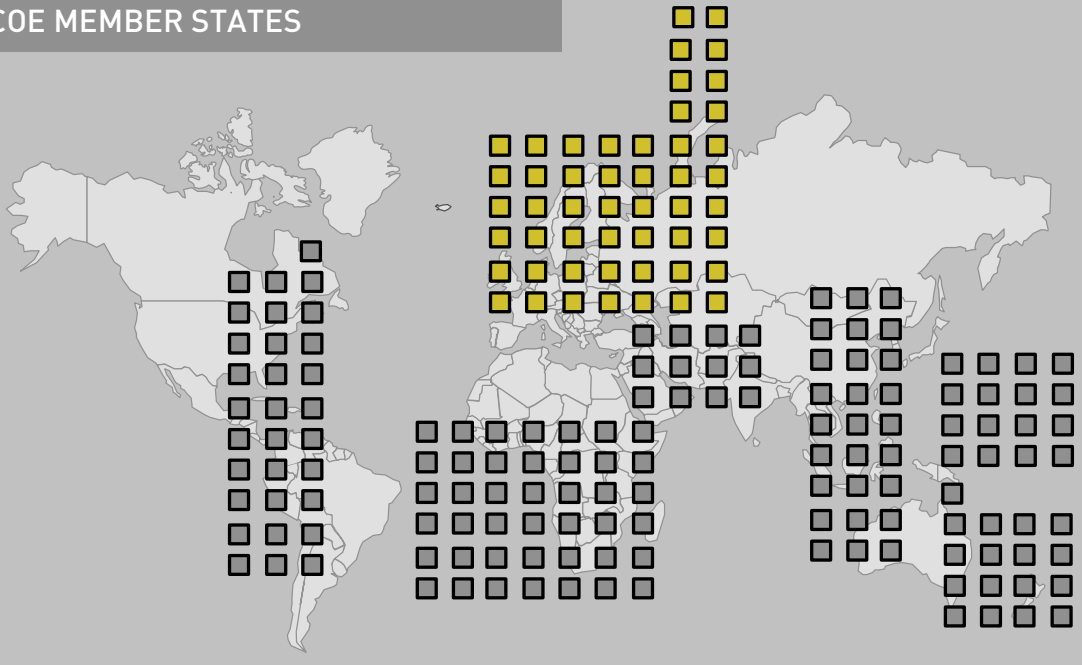
Cybercrime
Research Institute

UN MEMBER STATES

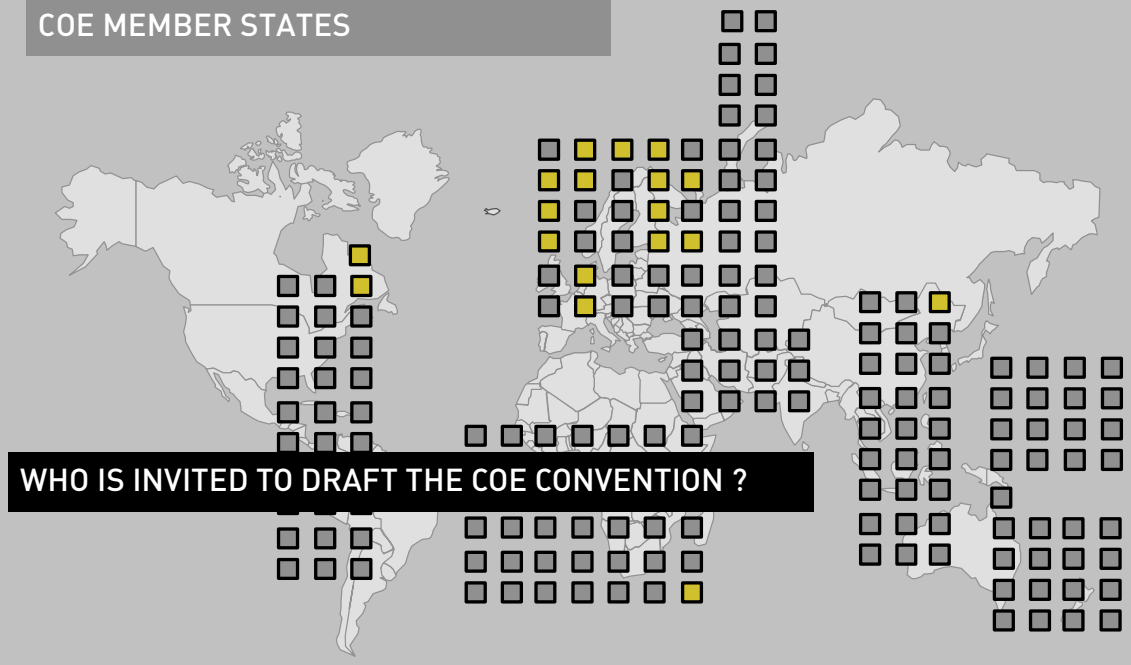


Cybercrime
Research Institute

COE MEMBER STATES

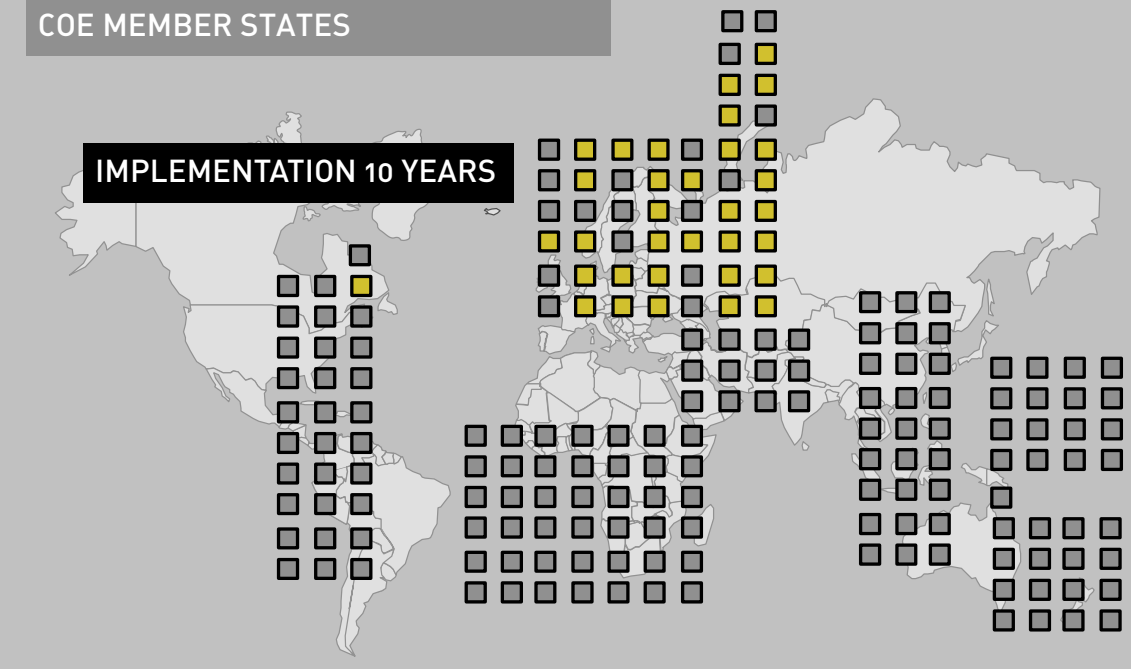


COE MEMBER STATES



WHO IS INVITED TO DRAFT THE COE CONVENTION ?

COE MEMBER STATES



IMPLEMENTATION 10 YEARS

Cybercrime
Research Institute

DONT COPY/PASTE FROM OTHER COUNTRIES AND REGIONS

Cybercrime
Research Institute

EXAMPLE: CHILD PORNOGRAPHY

- As cooperation requires legislation gaps can have significant impact
- In the early discussion about legal response to an online distribution of child pornography the drafter of regulations focused on digital images
- Today not only images and videos but also audio recordings of the sexual abuse of children are distributed online
- Older approaches often use language (such as "visually" or "image") that excludes such material

Convention on Cybercrime

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
a. a minor engaged in sexually explicit conduct;
b. a person appearing to be a minor engaged in sexually explicit conduct;
c. realistic images representing a minor engaged in sexually explicit conduct.

EU Directive Child Pornography 2011

(c) 'child pornography' means:
(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;

Cybercrime
Research Institute

EXAMPLE: CHILD PORNOGRAPHY

- As cooperation requires legislation gaps can have significant impact
- In the early discussion about legal response to an online distribution of child pornography the drafter of regulations focused on digital images
- Today not only images and videos but also audio recordings of the sexual abuse of children are distributed online
- Older approaches often use language (such as "visually" or "image") that excludes such material

Picture removed in print version
Bild zur Druckoptimierung entfernt

IOL News 2011

Picture removed in print version
Bild zur Druckoptimierung entfernt

US Training Manual

Cybercrime
Research Institute

EXAMPLE: CHILD PORNOGRAPHY

- ICB4PAC skeleton consequently avoids the term "visually"
- In addition the definition in ICB4PAC contains a clarification that audio material is included

ICB4PAC

(4) Child pornography means pornographic material that depicts presents or represents:
a child engaged in sexually explicit conduct;
a person appearing to be a child engaged in sexually explicit conduct; or
images representing a child engaged in sexually explicit conduct;
this includes, but is not limited to, any audio, visual or text pornographic material.

Cybercrime
Research Institute

BE MINDFUL THAT MORE IS NECESSARY THAN JUST LAWS

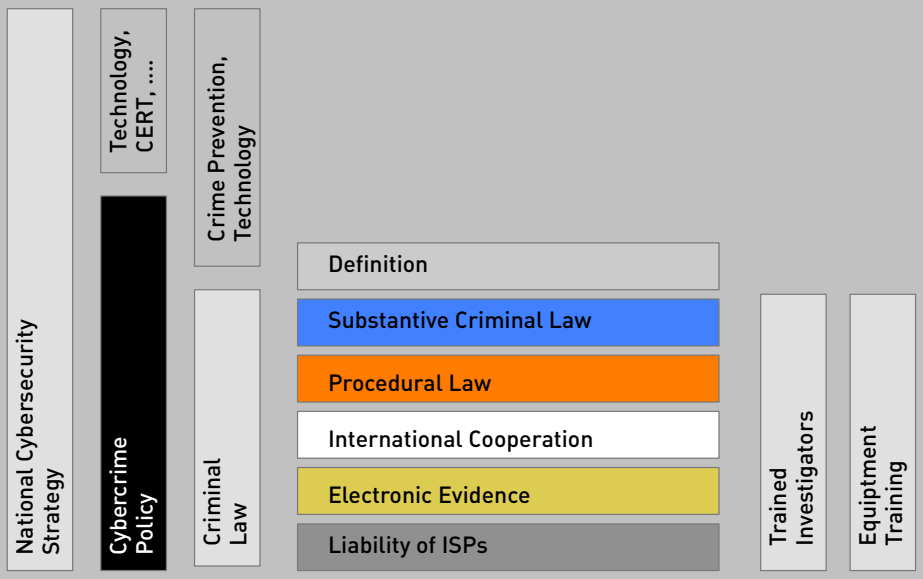
Cybercrime
Research Institute

COMPONENTS

Substantive Criminal Law

Cybercrime
Research Institute

COMPONENTS



Cybercrime
Research Institute

POLICY

- The relevance of a policy was highlighted during todays conference when the first speaker raised that in many countries different ministries "feel" responsible for the topic Cybercrime
- A cybercrime policy can address those issues

Cybercrime
Research Institute

FREE TOOLS


الاتحـــاد الدولـــي للاتصـــالات

فهم الجريمة السيبرانية:
دليـــل للبلـــدان الناميـــة

شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني
دائرة السياسات والاستراتيجيات
قطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات

مشروع أبريل 2009

للمزيد من المعلومات، يرجى الاتصال بشعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني، التابعة لقطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات، على العنوان التالي: cybmail@itu.int

الاتحاد الدولي للاتصالات

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFA.pdf

Cybercrime
Research Institute

Cybercrime Research Institute
Prof. Dr. Marco Gercke

Niehler Str. 35
D-50733 Cologne, Germany
gercke@cybercrime.de
www.cybercrime-institute.com