



STATE AGENCY
FOR INFORMATION TECHNOLOGY
AND COMMUNICATIONS
OF THE REPUBLIC OF BULGARIA



International
Telecommunication
Union

ITU Regional Cyber security Forum for Europe and the Commonwealth of
Independent States (CIS), 7-9 October 2008
Sofia, Bulgaria

Legal challenges of cyber crime, an overview

Judge Dr. Ehab Elsonbaty
Senior Judge in Damanhour Court,
Professor of Business Law, British University in Egypt

ehabelsonbaty@hotmail.com

ehabelsonbaty@bue.edu.eg





- ***The urgent need to deal with cyber crime.***





Why should we

care about cyber crime? 1

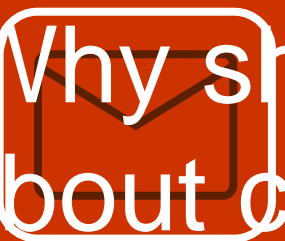


- Because it is a fashion?
- Because every body else does?
- Because it is merely very important and effects all levels of our life.
- Critical infrastructures: banks, governments, electricity, gas, water, traffic,
- chatting, mailing, shopping





Why should we



care about cyber crime? 2

- Endless assumption!
- The conclusion is: we are stoked to computer, internet and all other electronic mediums.
- Apparently IT IS HARD TO LIVE WITHOUT THEM!





- *General*

regulatory issues.



OLD WINE IN NEW BOTTLES OR NEW WINE IN OLD BOTTLES?

- Regulatory issues:
- Common law approach: minimum regulations – less litigations - self regulations.

Market leads

- Civil law approach: every thing is regulated – green / blue paper theory.
- Not used to codes of conduct, implementation guidelines..



Regulate or not to regulate, is this the question? 1

- CAUTION: online and offline
- Regulating means making INTERNET:
 - more functional,
 - less complicated and most importantly as safe and
 - reliable as possible.
- What to do,
- what not to do
- and how?
- Creating norms of behaviour.



Regulate or not to regulate, is this the question? 2

- We should not – while legislating for computers - bother by detailed technological issues,
- But rather a main frame which enables the law to adopt the best technology exists in the field in order to apply its provisions properly.



Regulate or not to regulate, is this the question? 3

- The ability of the legislations of many states to govern computer activities properly is under question thanks to the rapid development of technology which cause new problems on a speed regular bases.
- The interaction problems between technicians and lawyers.





- **Substantial**
challenges of cyber
crime.



Challenges to substantive rules!



– Computers may be a tool (instrument)/fraud or incidental to an offence, but still significant for law enforcement purposes /saved data or subject (target) to crimes?





Classical crimes! 1



–A-Computer related crimes:

- Theft.
- Fraud.
- Industrial espionage.
- Facilitation of prostitution.
- Forgery.
- Terrorism.
- Spying.





Classical crimes! 2



- Spreading of e – banking.
- E-Money.
- Smart cards.
- employee and employers.
- Money laundering.
- Gambling with illegal cash.





Classical crimes! 3



- B- Content related crimes:
- The information and the data which are processed by computers are most of the times much more valuable than the hardware itself.
- Copy rights.
- Stalking,
- Harassment,
- Hate Speech.
- Offences against Morality.





Classical crimes! 4



- Our existing legal systems can accommodate this type of computer related crime in many cases.
- It would be better that some articles in the penal code be modified in order to make this accommodation process nice and easy for all the interested parties such as law enforcement bodies and judges.



C- Computer sabotage crimes 1

- This type of cyber crimes covers the crimes which affect the:

- security,
- integrity,
- confidentiality,
- reliability and
- availability of computer systems.



C- Computer sabotage crimes 2

- Unauthorised access to computer systems:
- Unauthorized access:
- Unauthorized access with out committing crimes.



C- Computer sabotage crimes 3

- Unauthorized access with the intention to commit another crime:
 - Copy – send.
 - Unauthorized modification.
 - Delete.
 - malwares.
 - viruses.
 - DOS.
 - Compromise.
 - spam.
 - Improve?
 -



C- Computer sabotage crimes 4

- Unauthorized modification.
- Delete.
- malwares.
- viruses.
- DOS.
- Compromise.
- spam.
- Improve?



New trends in cyber crime!

- Phishing.
- Vishing.
- Farming.
- smishing.





- **Challenges to procedures rules in the field of criminal matters.**



Challenges for procedures and law enforcements! 1

- It is very volatile, easily unintentionally altered without obvious trace, and it is highly novel, creating problems not only of explanation but also of forensic testing.

- Computer forensics is a reasonably well-established subject area, but unlike most forms of forensic science many of its techniques have not been around long enough to have been properly tested by peer-reviewed publication.

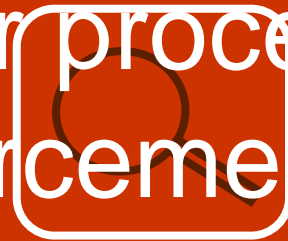


Challenges for procedures and law enforcements! 4

- Legitimizing the activities of the various units that investigate and prosecute computer crime.
- This should cover:
 - new means of scrutinising activity on the internet,
 - use new and advanced techniques to recover data from seized computers and data media,
 - and seek to infer actions and intent on the part of defendants by interpreting the way in which a computer may have been set up and, over a period, used.



Challenges for procedures and law enforcements!



5

- Ensure that the police force has the required resources and expertise to handle the investigations.
- Training for police officers should cover all the related area of forensic issues of computer crime such as searching, seizing, recording, intercepting...etc.
- Training of prosecutors, judges and legislators.





- ***The need to new trends of international cooperation in criminal matters.***



Challenges to International co-operation



- Cyber crime is a cross border crime.
- Inconsistent legal responds.
- No single organization or body is able to fulfill the task
- The biggest challenge is not only to obtain evidences.
- Rather it is how you do this respecting both of the legal systems.





- ***The way forward.***



International cooperation and harmonization 1



- The classical criminal co-operation between the countries is not capable of handling this type of crime, this classical co-operation may take months to conduct a procedure in another country or to operate a particular investigation on the territories of different jurisdictions.

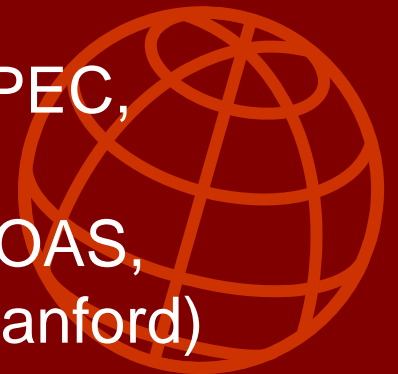
- Mechanisms of co-operation across national borders to solve and prosecute crimes are complex and slow.



International cooperation and harmonization 2



- United Nations UN,
- International Telecommunication Union ITU,
- European Union EU,
- Council of Europe COE,
- The commonwealth,
- Organization for Economic Co-operation and Development OECD,
- The Interpol,
- The G8 Group of States,
- COMESA,
- Asia Pacific Economic Cooperation APEC,
- ASEAN Group of States,
- The Organization of American States OAS,
- Universities and research institutes (Stanford)



International cooperation and harmonization 3

- It is time to reconsider the traditional separation between civil laws and common laws.
- the threat is united.
- The evidences are be default crossing borders.
- the gap is not that big.
- At any rate, we have to sort out a way that mutual legal assistance is speeded up and are legitimate for both of the countries.





- **Conclusions & recommendations**

=





Conclusions



- 1- Computers are very important in our life and this importance will increase. There is an urgent need to assure that the integrity, confidentiality, availability, reliability and security of computer systems and networks.





Conclusions 2



- 2- This explains the need to regulate computer crimes – and all the other related areas - such as Internet and e-commerce – comprehensively,
- Specially that one of the main functions of any law is a protective one.



Conclusions 2

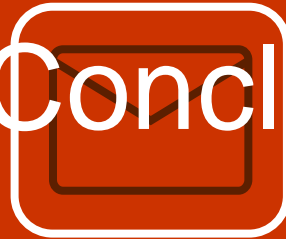


- 3- Updating the criminal law is needed to accommodate the particular nature of cyber crime.
- This updating may be done by
 - modifying some articles regarding the classical crimes done via new mediums,
 - abolishing some others which are not adequate completely, or even
 - by creating new rules to the completely new issues.
- 4- The levels of punishment either by imprisonment or fining should be reviewed and this also goes for the accomplices.





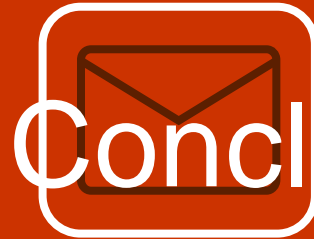
Conclusions 3



- 5- A successful updating for the law should secure that the civil remedies are given in the cases of computer crimes.

6- Training is extremely important, not only for law enforcements and prosecutors but also for judges and legislators.





Conclusions 4

- 7- The international nature of cyber crime creates the need to an international solution which should cover:
 - substantive,
 - procedures and
 - international co-operation rules.





STATE AGENCY
FOR INFORMATION TECHNOLOGY
AND COMMUNICATIONS
OF THE REPUBLIC OF BULGARIA



International
Telecommunication
Union

ITU Regional Cyber security Forum for Europe and the Commonwealth of
Independent States (CIS), 7-9 October 2008
Sofia, Bulgaria

**@ Thank you for your attention,
@ questions or comments?**

Judge Dr. Ehab Elsonbaty
Senior Judge in Damanshour Court,
Professor of Business Law, British University in Egypt

ehabelsonbaty@hotmail.com

ehabelsonbaty@bue.edu.eg

