



Common Market
for Eastern and Southern
Africa



International
Telecommunication
Union

ITU Regional Cyber security Forum for Eastern and Southern Africa, 25-28 August 2008. Lusaka, Zambia

Legal Foundations To Combat Cyber Crime

Judge Dr. Ehab Elsonbaty
ehabelsonbaty@hotmail.com
ehabelsonbaty@yahoo.com



Elements of discussion



- The urgent need to deal with cyber crime.
- General regulatory issues.
- How may our legal system respond to cyber crimes.
 - Substantial issues.
 - Procedural issues.
- The current rules in the Egyptian legal system for cyber crime.
- The need to new trends of international cooperation in criminal evidences.
- The Egyptian approach.
- The way forward.
- International instruments/ abandoning the gap between legal systems.
- Conclusions.





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





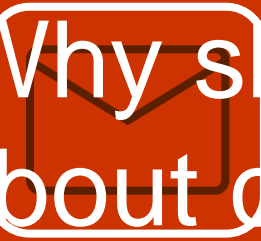
“..Our national security will be in risk if we do not protect our electronic networks and systems..”



AL PACINO TO COLIN FARRELL
- THE RECRUIT, 2002



Why should we



care about cyber crime? 1



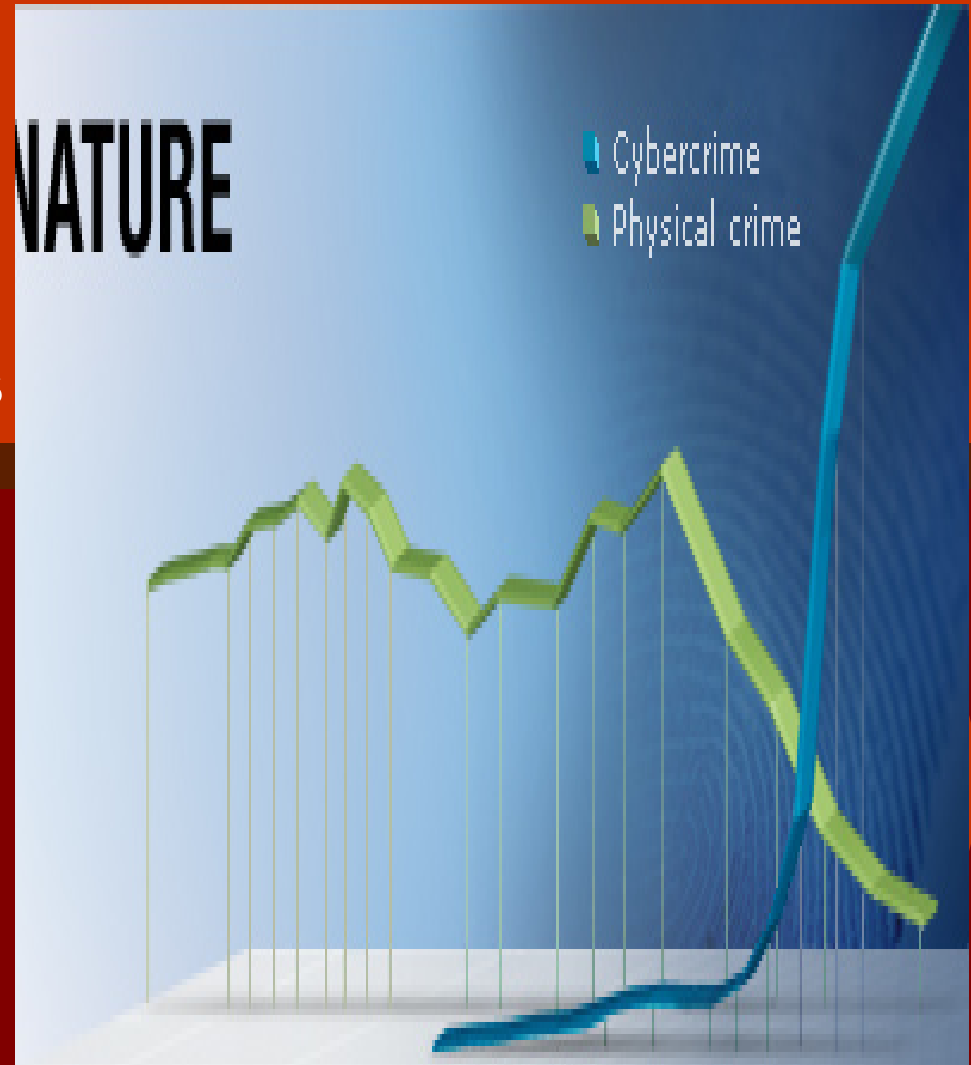


Why should we

care about cyber crime? 2

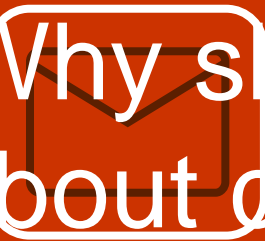


- Because it is a fashion?
- Because every body else does?
- Because it is merely very important and effects all levels of our life.
- Critical infrastructures: banks, governments, electricity, gas, water, traffic,
- chatting, mailing, shopping



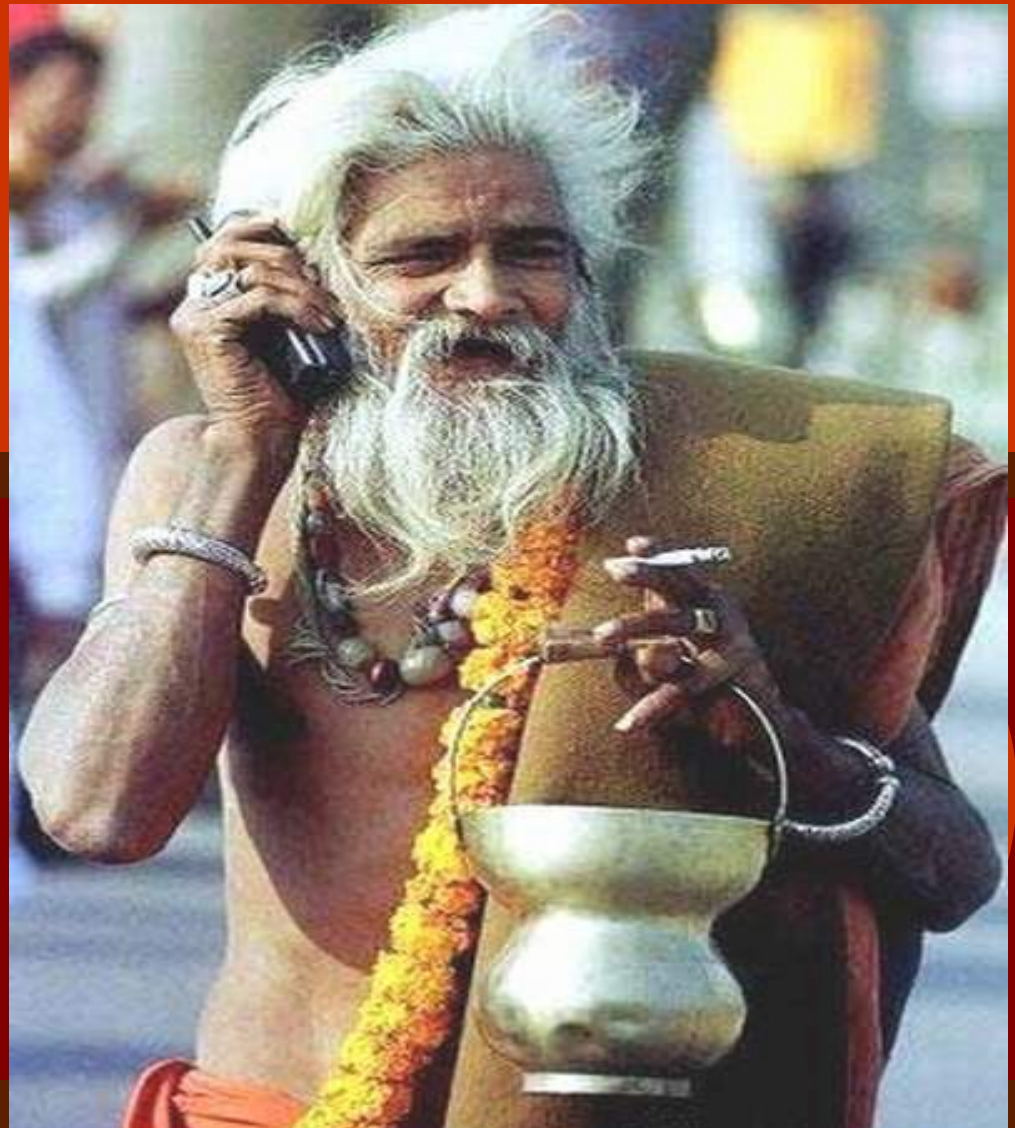


Why should we



care about cyber crime? 3

- 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.



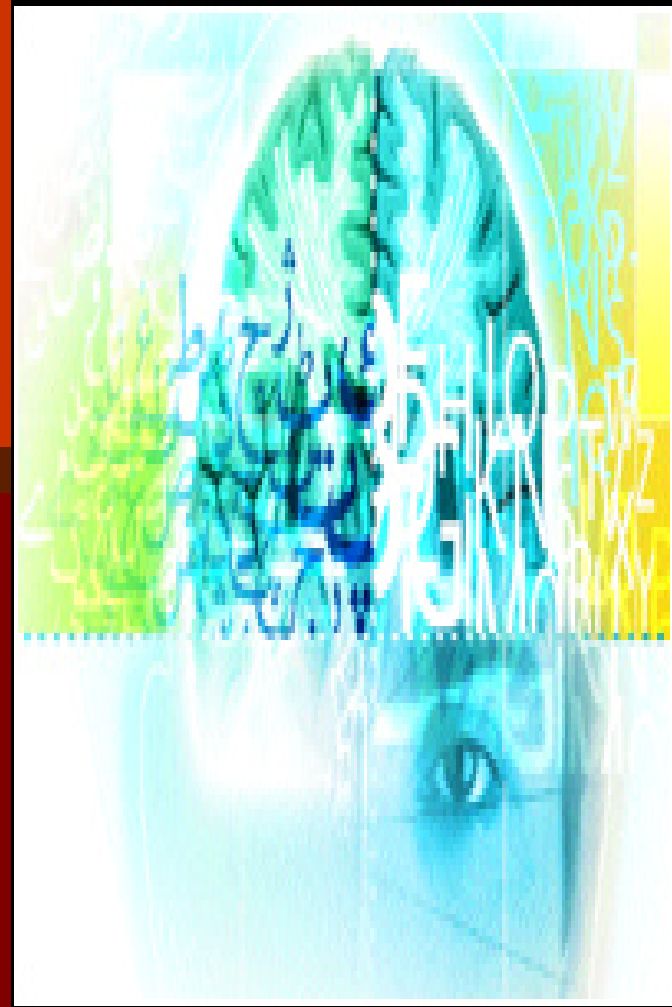


- ***Substantial challenges of cyber crime.***



Clarification of definitions

- Cyber Crime.
- Internet Crime.
- Computer Crime.
- Hi-tech Crime.
- Information Technology Crime
- OVER, ON, THROUGH, WITH computers, mobiles and Internet.



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.





Classical crimes! 2



- Our existing legal systems can accommodate this type of computer related crime in many cases.
- It would 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.





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.



'Sir, somebody in my class has stolen my games CD!'



Classical crimes! 4



- the difficulties posed by computer content crimes are ones that can be remedied relatively easily by amendments to the laws.
- This should include giving a wider scope of some definitions such as what may be considered a copy of a photograph.



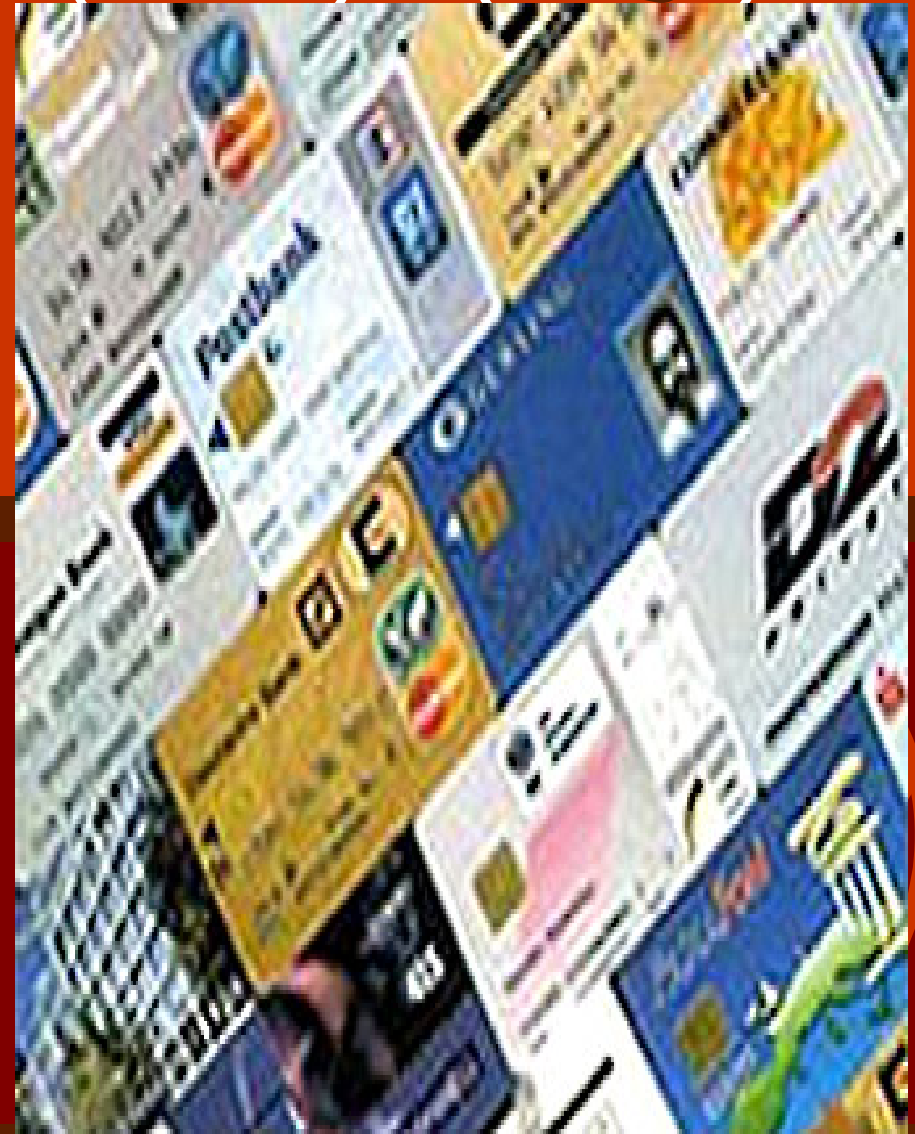


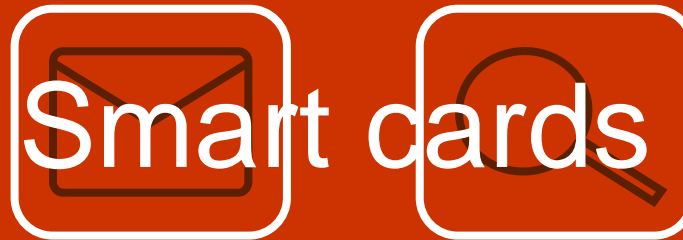
- Spreading of e – banking.
- E-Money.
- Smart cards.
- Money laundering.





- By its decentralized, distributive nature, electronic money has the same potential for transforming economic structure as personal computers did for overhauling management and communications structure .



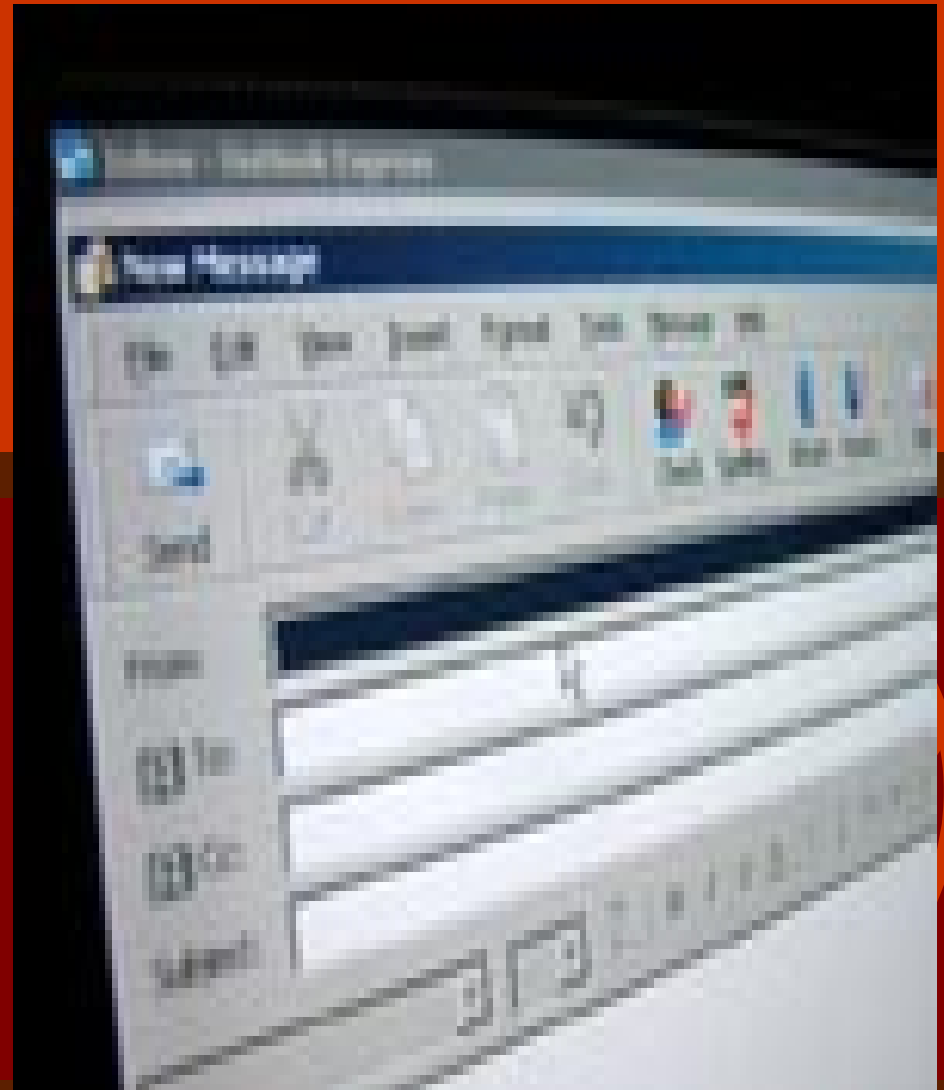


- What should be protected?
- The smart card itself?
- The design?
- Or the application on the card?
- Is minimum level of security is required to grant protection?



Employer and employees ! 1

- Should be regulated.
- Dangers may occur.
- Privacy.
- Normal post mail.
- Monitoring e-mails?
- Monitoring phone calls?
- Should be informed.



Employer and employees ! 2

- how long?
- How many times?
- different international applications?



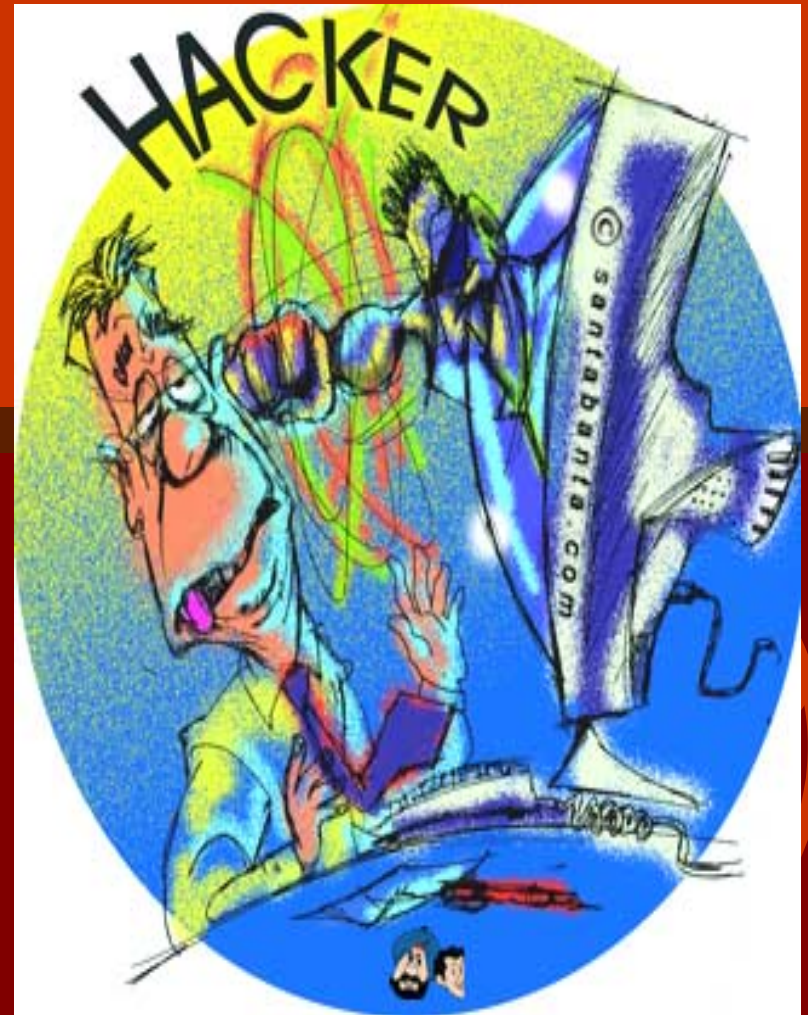


Sabotage!



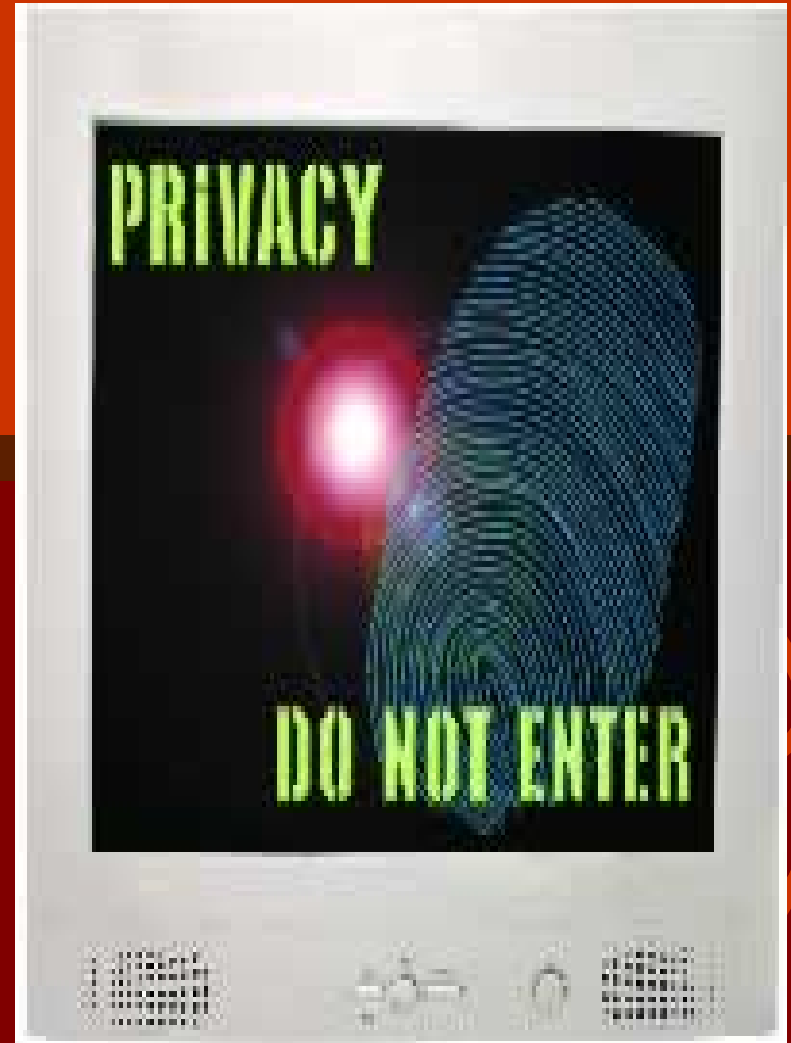
C- Computer sabotage crimes 1

- 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.

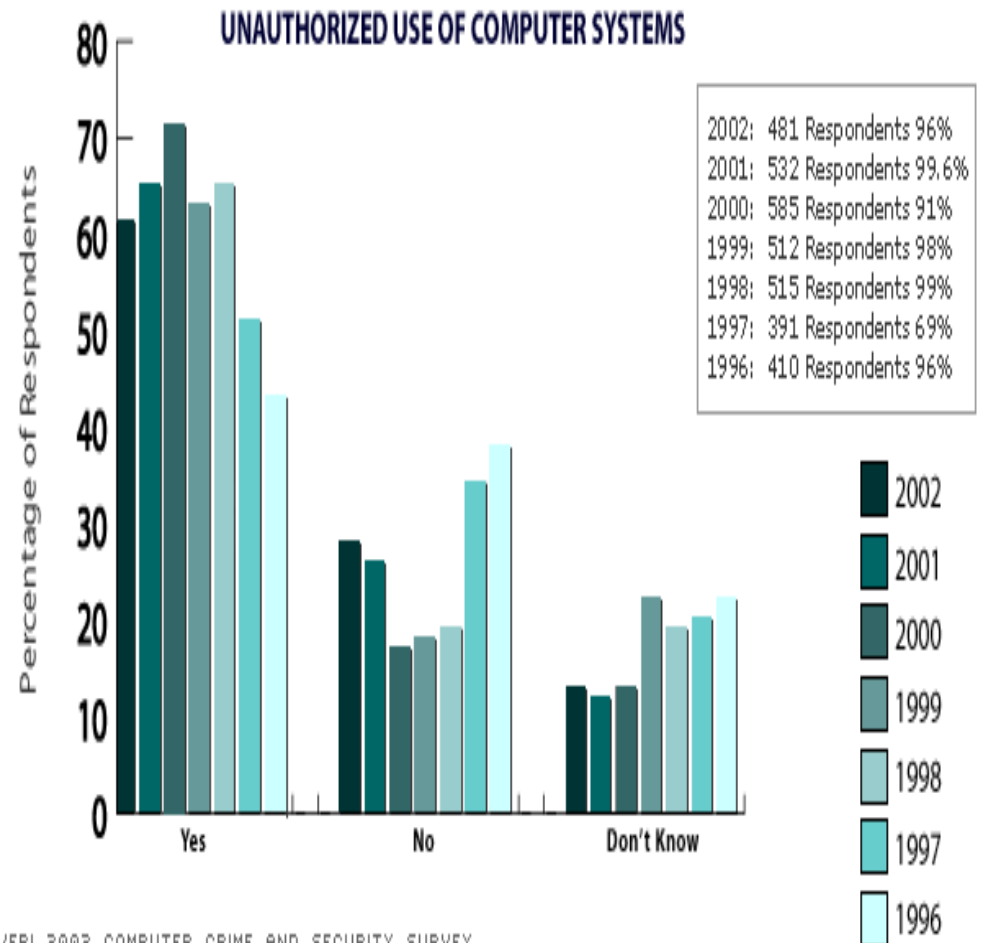


C- Computer sabotage crimes 3

- Unauthorized access with the intention to commit another crime:
- Copy – send.

CYBERCRIME 2002 RESULTS

NEXT >



CSI/FBI 2002 COMPUTER CRIME AND SECURITY SURVEY
SOURCE: COMPUTER SECURITY INSTITUTE

C- Computer sabotage crimes 4

- Unauthorized modification.
- Delete.
- DOS.
- Compromise.
- Improve?



New trends in cyber crime!

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





- ***The current rules in the Egyptian legal system for cyber crime***





- **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! 2

- Needs not only a law to draw the procedures to be followed in computer crime but also to develop sort of Quality Assurance protocols that are used in more established areas of forensic science.



Challenges for procedures and law enforcements! 3

- A simple way of procedural regulation may be an article,
- Which provides for the search of any premise and seizure of any evidence with a warrant, if there is reasonable cause to believe that an offence under the Act has been committed.



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.



Challenges for procedures and law enforcements! 6

- Prosecutors should be trained to carry the proof of electronic evidence to the court and stand strongly behind them.
- Trained about the limits they should give their warrants within, in a way that assure a flexibility of movement for the police and maintain the basic human rights of the accused.
- Judges and legislators!



Challenges for procedures and law enforcements! 7

- Training between the theory and the practise.
- Who should design the training?
- How may the training be conducted?
- The crucial partnership with the private sector?
Investments- tools
High expectations of the judiciary?



Challenges for procedures and law enforcements! 8



- Cyber cafes:
- Situation in Egypt.
- Example from Italy.
- WIFI:
- Coffee shops.
- Companies.
- Houses.





- **Focus on the**
Egyptian legal
system.





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





The Potential for E-money Laundering



- The abuse of e-money by money launderers may become a significant problem in the future because e-money systems will be attractive to money launderers for two reasons:
- transactions may become **untraceable**;
- and transactions are **incredibly mobile**.





Money laundering in cyberspace



- In a tactic as old as banking itself, criminals have always used banks as a sure-fire way to launder money gained through illegal means.
- But with the advent of internet banking, "following the money" to locate and prosecute money launderers and criminals has become more difficult than ever.





Money laundering in cyberspace 2



- Money laundering, which involves disguising the origins of illegally obtained cash and then transforming it into apparently legitimate investments, is bolstered by the near anonymity that can sometimes be achieved through internet communication.
- Internet banks allow for access to accounts from anywhere in the world" A potential risk exists at any stage of the contact between a new customer and a financial institution," (FATF).





Money laundering in cyberspace 3



- According to FATF:
in the case of internet banking, the difficulties "are increased if the procedures for opening [accounts] are permitted to take place without face-to-face contact..."

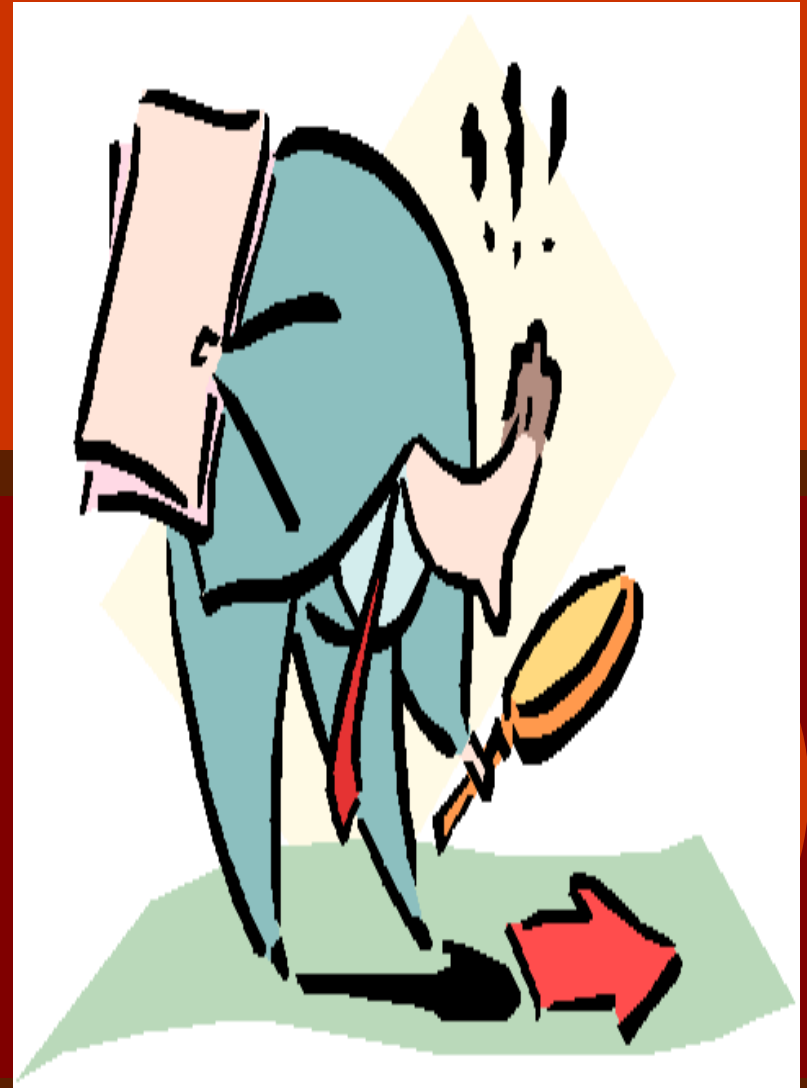




Money laundering in cyberspace 4



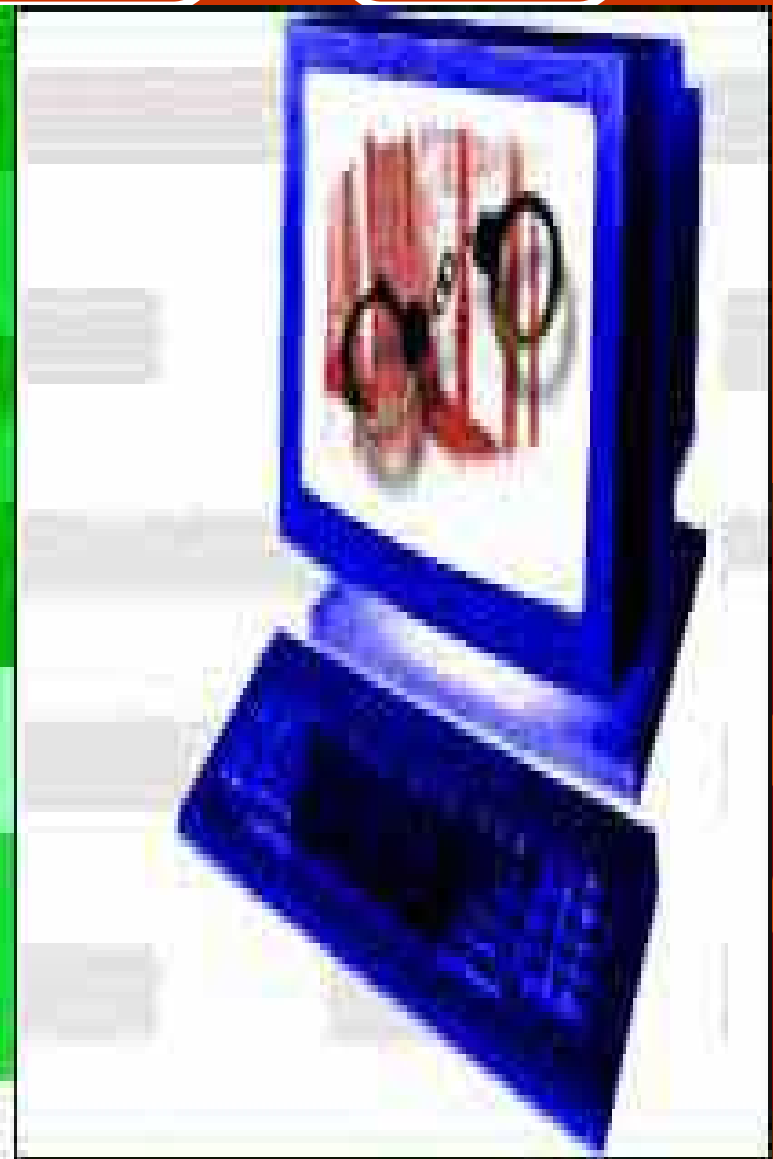
- FATF, also noted that worldwide access further complicates detection of fraud.
- It is not always clear whether an account is accessed from a country other to where the money is held, and account managers may simple be too busy to monitor all the activity of individual account holders.



Gambling with illegal cash ¹

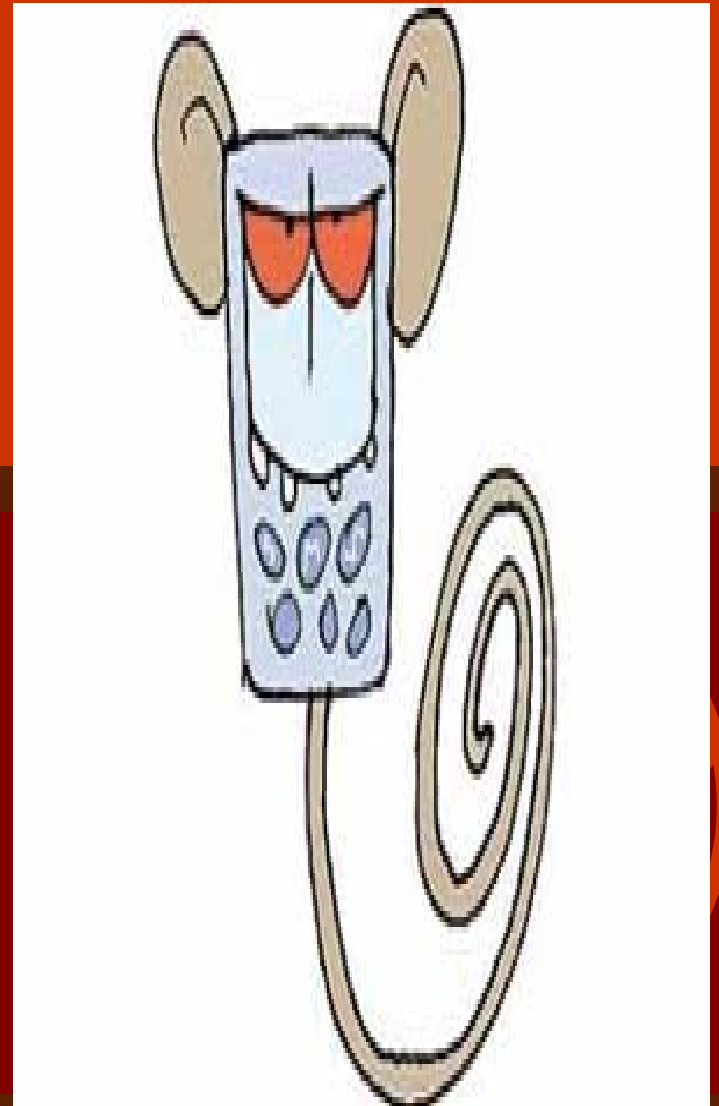


- Internet-based gambling operations can act as a haven for illegal cash-washing operations.
- The FATF said there is evidence that criminals are using online casinos to commit crimes and launder the proceeds.



Gambling with illegal cash 2

- Online casinos further complicate tracking of questionable transactions because gambling records are software based and at the gambling site - often located offshore.
- That makes evidence gathering more difficult because the records are harder to find and may not exist at all.



Challenges to International co-operation



- The biggest challenge is not only to obtain evidences.
 - Rather
- It is how you do this respecting both of the legal systems.





- *The Egyptian approach.*





- ***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

- Needs instruments and networks.
- On the international level:
 - UN conventions against organized crime and corruption.
 - European conventions.
 - European arrest warrant.



International cooperation and harmonization 2



.COE CONVENTION 2001 ON CYBER CRIME.

- it covers:
- 1- substantial rules (criminalization)
- 2- Procedures.
- 3- International co-operation.
- 24/7 network.
- G8.
- INTERPOL and EUROPOL.
- Cases studies.



International cooperation and harmonization 3

- Model laws and guidelines:

- Various organizations have recognized the inherently trans - border nature of cyber crime, the ensuing limitations of unilateral approaches, and the need for international harmonization of legal, technical, and other.

- The European Council, The Organization for Economic Co-operation and Development OECD, the European Union, the Interpol and the G8 group.



International cooperation and harmonization 4


- Good news!
Establishing the International Virtual Forum against Cyber Crime.
- Training of Law enforcements, prosecutors and judges.
- Portal for cyber crime.
- Two pilot projects.
- Resources and fund.



International cooperation and harmonization 5



.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**

=

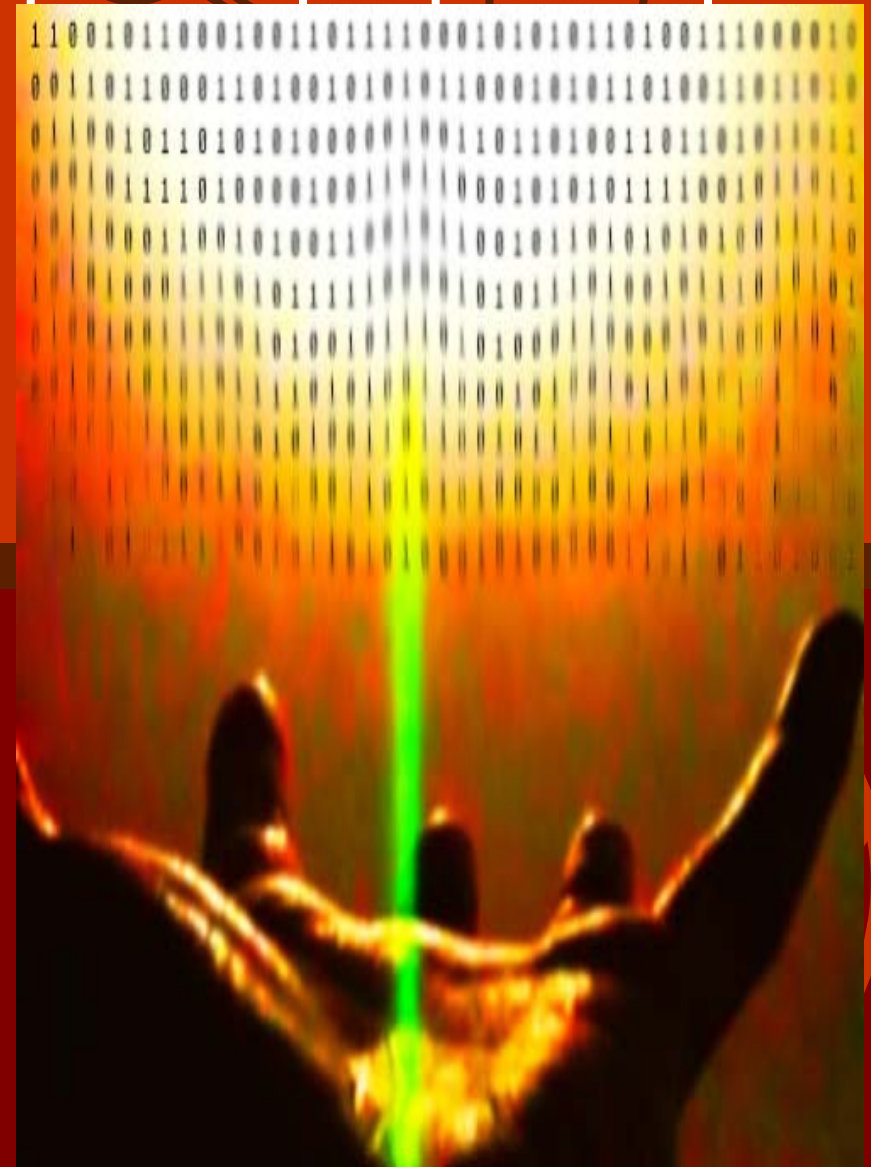




Conclusions 1



- 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 3



• 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.



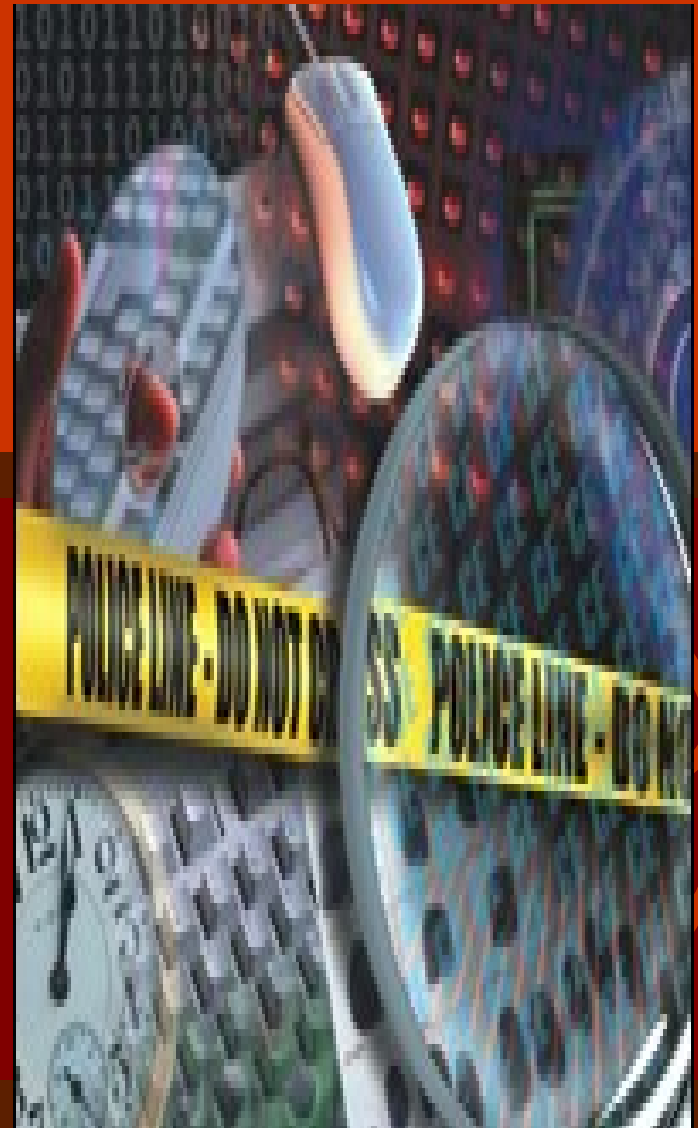


Conclusions 4



- 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.

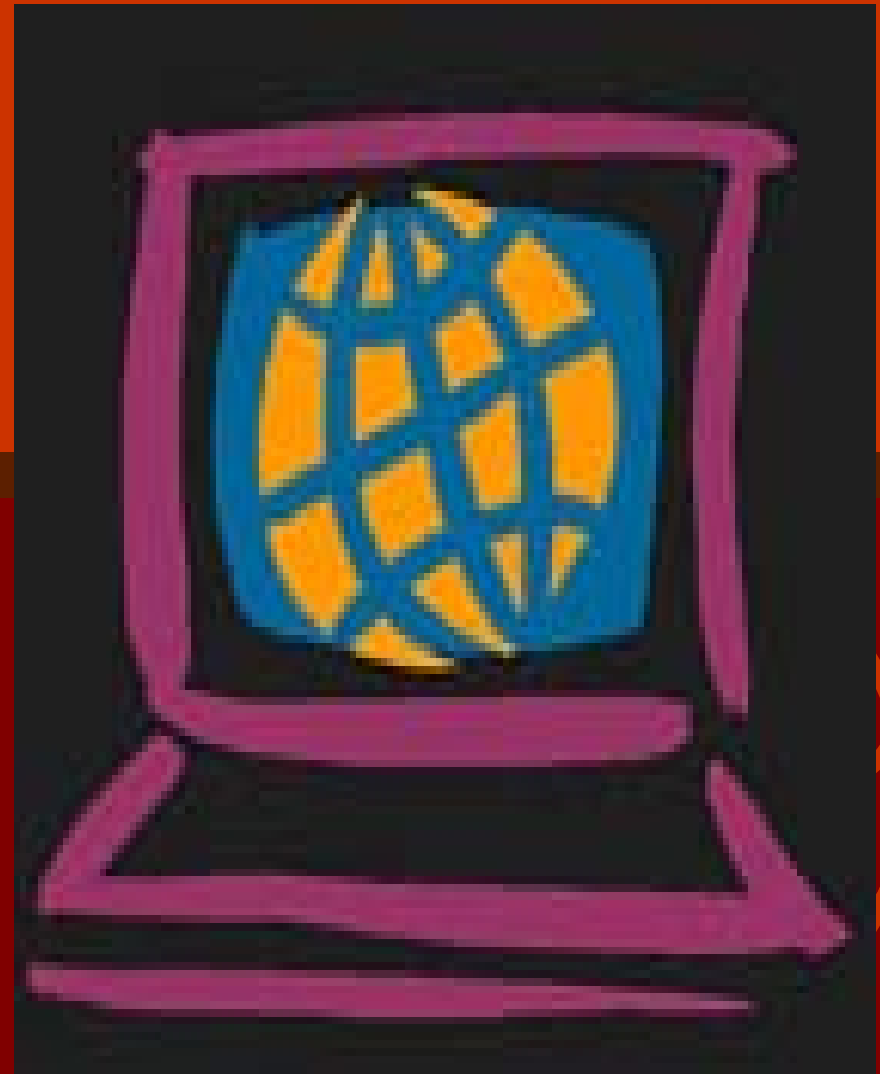




Conclusions 5



- 7- The international nature of cyber crime creates the need to an international solution which should cover substantive, procedures and international cooperation rules.
- 8- Looking forward to a modern Egyptian cyber crime act.





CONCLUSION



They are
clever!



**BUT WE ARE
BETTER!**





Common Market
for Eastern and Southern
Africa



International
Telecommunication
Union

ITU Regional Cyber security Forum for Eastern and Southern Africa - 25-28 August 2008. Lusaka, Zambia

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

Judge Dr. Ehab Elsonbaty
ehabelsonbaty@hotmail.com
ehabelsonbaty@yahoo.com

