



# Estonian experience in fight against cybercrime

Markko Künnapu  
Ministry of Justice of Estonia



# Legislation I

## amendments to the Criminal Code 1997

- separate chapter – separate category
- all the main aspects of cybercrimes were covered
- public computer systems and registers
- computer systems containing classified information
- private computer systems



# Legislation II

## new Penal Code 2002

- computer crimes as part of the crimes against property
- no difference between public and private property
- the rest of the regulation was kept the same



# Meantime

- Estonia ratified the Convention on Cybercrime in 2004
- problems at national level with the implementation
- regulation was limited and too restrictive
- analysis was needed, but there was no interest for that



# IT solutions

- increasing number of different IT solutions
- digital signature
- e-banking
- e-government
- e-voting
- e-taxboard, e-customs, e-police etc
- dependancy on Internet
- vulnerabilities – no particular attention





Hacked from RUSSIAN HACKERS (thx to ZyklonTeam , S-Teals, Web-Hack)

Our Honour

Our Freedom

Our Victory ...



thx 2 sites : DESANTNIK.mindmix.ru, S-Teals.ORG, Antichat.RU, ZyklonTeam.org, NNM.RU, Web-Dozor.ru, ХАКЕРЫ.ru, 0x48k.cc, taxidermia.void.ru







# Legislation III

## amendments to the Penal Code 2008

- legal clarity
- obstacles removed
- punishments increased
- compatibility with international instruments
- cybercrime as threat to economy and national security
- CI – new aggravated circumstances introduced
- cyberattack as a terrorist crime



# Case law examples



# Story of an angry customer

- A.B. 44 year old male
- DDoS attacks in 2004 – 2007
- Targets were:
  1. computer vendor
  2. internet service providers
  3. insurance company
  4. online media company
- different motives
- damages more than 400 000 EUR



# Genealogy of a criminal

Sergei Tšurikov

## 2002 – phishing attack

- IT student
- targeted against local bank and its customers
- used a cyber cafe to send large amount of e-mails
- created a fake bank website and victims were asked to enter their online banking codes
- attempted to transfer money from victims' accounts
- was arrested one day later



## 2005 – phishing attack against banks in Germany

- used a Trojan that was sent to german citizens by e-mail
- collected online banking user names and passwords
- transferred money to bank accounts in Estonia (mules)
- total damages 179 727 EUR
- as some transactions were returned the criminals could get hold only 115 780 EUR



## 2008 – attack against RBS Worldpay

- acted with a group of 3 persons
- used hacking to compromise the data encryption system
- counterfeit debit cards for network of “cashers”
- increased the account limits
- 4 debit cards in Estonia
- 08.11.2008 from 9.00 to 18.53 3 persons withdrew 226 895 EUR



- started worldwide at the same time
- 2100 ATM-s, 280 cities in US, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, Canada
- 9,4 million USD in less than 12 hours



Thank you!