Criminal Justice System’s Intervention to Cybersecurity Threats: Panacea or Pandora's Box?

Aleš Završnik, LL.D.
ICT and Crime

1. New forms of crime
   - old wine new bottles (Grabosky)
   - new wine no bottles (Wall): information, computers, networks

2. New response to crime
   - Prevention
     CCTV, biometry (ex. automatic face recognition), passenger control
     (ex. Passenger Name Records), data retention ⇒ databases booming
   - Reaction
     - institutional rearrangements
       new police/prosecution forces, e-justice (case management systems,
       videoconferencing, computer animation, virtual environments)
     - new arrangements of order-maintenance
       (public-private partnerships, internet governance)
ICT and Crime

1. new forms of crime
   ⊳ substantial criminal law challenges
      - taxonomies of cybercrimes

2. new reaction to crime
   ⊳ procedural criminal law challenges
      - digital/cyber/computer/network-forensics
      - jurisdiction
      - evidential issues
SERIOUSNESS AND HARM

Cybercrime
v.
Reaction to cybercrime
1. THE PROBLEM OF A “PROBLEM” BE AFRAID ARGUMENTS

Report from the Council of Europe, Octopus Interface 2007

(1) Information societies worldwide increasingly dependent on ICT and the growth of cybercrimes renders societies highly vulnerable.
(2) Malware evolving and spreading rapidly
(3) Spam majority of email traffic and carrier of malware
(4) Botnets tools of organized cyber crime
(5) An underground service economy
(6) The threats are changing: the mass, multi-purpose and global attacks replaced
(7) Sexual exploitation and abuse of children and human trafficking
(8) Attacks against the critical information infrastructure on the increase
(9) P-2-P networks
(10) Damage caused 50 milliard dollars a year
2. THE PROBLEM OF A “PROBLEM”
“BUT WHY?” ARGUMENTS

1. few “official” sources (distributed environment undermines conventional methodologies for collecting data)
2. dubious automated reports (cookies & spyware)
3. individually not serious (aggregate volume)
4. victim data & offender data
5. incidents reported v. known prosecutions
6. what ought (risk assessment) v. what is (reality)
2. THE PROBLEM OF A “PROBLEM”
WHAT IS CYBERCRIME?

1. the legislative discourse about cybercrime
   what is supposed to happen?

2. the academic discourse
   what has happened?

3. the expert knowledge
   what is actually happening?

4. the popular/layperson’s discourse
   what the person on the street thinks is happening?

2. THE PROBLEM OF A “PROBLEM”
WHAT IS CYBERSECURITY?

1. protocol security (IETF)
2. protecting the network (CERTs)
3. making it safe to do business
4. a state’s sovereign interests
5. of users’ human rights

© Avri Doria (2007). What do the Words “Cyber Security” Mean?
In: The Power of Ideas, Kleinwächter W. (ed.)
3. THE PROBLEM OF THE CRIMINAL JUSTICE REACTION TO “THE PROBLEM”

3.1 substantial criminal law

a) Content crime
   - child pornography: virtual & realistic images
   - extreme & violent pornography: consent, adults
   - “terrorist” publications
   - Nazi paraphernalia, Holocaust denial sites

Tendency:
   - content control strategies (technical filtering) referring to only limited crimes but grant law enforcement powers across all types of computer crime
   - Internet filtering: flowed+HRconcerns+inovation/creativity
3. THE PROBLEM OF THE REACTION

3.2 substantial criminal law

b) Infringement of IP rights

- Criminalising the vast majority of users
- Temporary (always on-line connection \( \Rightarrow \) easier to subscribe than be a database manager)
- Damage (dubious) and types of users (manifold)
- Reaction:
  - “The Three-Strike Scheme” (warnings \( \rightarrow \) cutting subscriptions)
  - contribution from ISPs (~ cable and satellite royalties)
3. THE PROBLEM OF THE REACTION

3.3 substantial criminal law

c) Modes of execution (actus reus): possession v. procuring/supplying
   • cache memory
   • deleted but recoverable files
   • P2P: illegal copy in My Shared Folder (Kazaa) / Shared Files (eMule)

d) Organized crime and terrorism
   Computer plays a secondary role

e) Identity theft
   Anecdote-based policy as something has to be done
3. THE PROBLEM OF THE REACTION

3.4 procedural criminal law
Cyber-forensics

Electronic footprints:
- how to **collect** intangible, transient data,
- **analyse** and make sense
- **preserve** digital information?

1. **Identifying suspects**: data → virtual identity → real person
   (IP address – assigned CSP – user – subscriber’s account)
2. **Obtaining data**: transmitted, residing on a resource
   (types & modes of storage (logical, physical level), deletion and integrity problem)

**Problems:**
- deregulation of expertise: who can be a cyber forensic? registration of forensic practitioners, guidance on treatment of digital evidence
- training of law enforcement personnel: offered by manufacturers of forensic tools?
3.5 procedural criminal law
Cyber-forensics techniques

Cyber-surveillance
- targeted – covert v. non-targeted – transparent (monitoring, filtering)
  - the role of CSPs in state-instigated surveillance: imposed obligations and voluntary self-regulation (blocking sites in search engines)
  - commercial interests of CSPs (ex. competing internet telephony, profiling of customers)

Surveillance Interception (CSPs derived)
- data transmitted by suspects (content data):
  transmitted & stored, public services/networks? Costs?
- data generated by CSPs (communications data):
  problems:
  - different definitions of data amongst countries
  - distinguishing: communications v. content data (sequence no. of packets)
  - the extent of obligations to disclose data (in possession, capable of obtaining)
  - relevant authority: public v. private, which data, in which phase
  - data retention of transient data: 90 days (Convention) v. 2 years (Directive)
  trends: new capabilities for retention, extended data types (traffic data, usage data, subscriber data)

Search & seizure (suspect derived)
- warrant: the extent of entry authorisation (ex. Domestic wireless networks)
- the scope of the warrant regarding material contained on the disk
- protected data (access, conversion)
3.6 procedural criminal law
Evidentiary rules

How to evaluate digital data as existing law tailored to gathering of physical evidence and eyewitness testimony?

ex.: search warrant for digital evidence is a two-stage process:
(1) a physical search to seize computer hardware,
(2) execution of a second electronic search to obtain the data from the seized computer

Effect
ICT challenge traditional procedural concepts:
shift in favour of law enforcement
3. THE PROBLEM OF THE CRIMINAL JUSTICE
REACTION TO “THE PROBLEM”

Conclusion:
Over-extension of the reach of criminal law

Impact on civil liberties – human rights concerns
- Privacy
- Freedom of expression
- Freedom of association
- Fair trial

Impact on free use of Internet – public policy concerns
- Data retention: impact on operators and consumers
  • 73% heard about the data retention,
  • 11% did not use the phone/e-mail because of that
  • 6% considers that they received less info
  • 52% that would not use telecommunications services for:
    discussion with pharmacists, psychotherapists, marriage brokers
The Problem

cybercrimes

v.

Reaction to “the problem”

criminal justice system’s response

Which threatens us more?
Thank you for your attention!

Aleš Završnik, LL.D.

ales.zavrsnik@pf.uni-lj.si