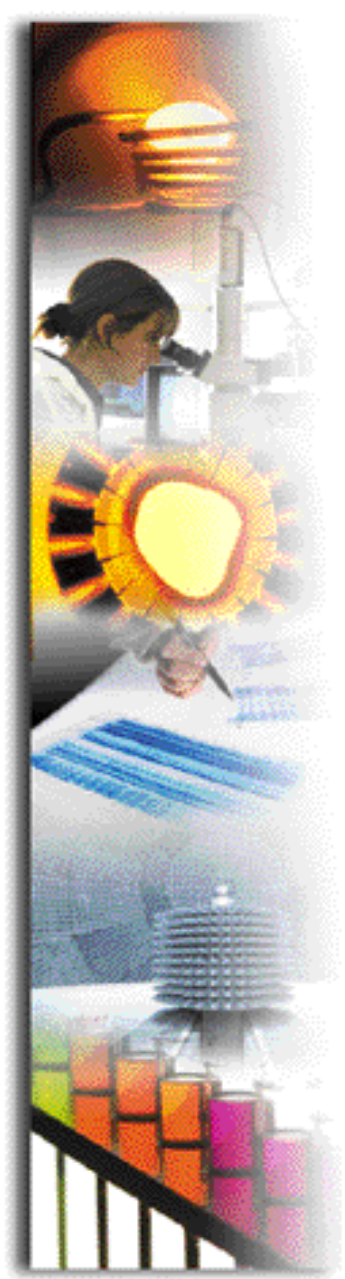


JRC

The challenge of electronic evidence – the European response

Neil Mitchison

Neil.Mitchison@jrc.it

Why is electronic evidence important?

- In the on-line world:
  - lack of trust is a major barrier to expansion of e-services
  - trust depends on being able to establish what happened
  - a proof-free Internet means a law-free Internet
- Off-line: increasingly, **all** major investigations involve electronic evidence

And so ...

- Electronic evidence is easy to create ... in fact, much too easy.
- No one trusts the evidence itself
- Two current solutions:
  - the “wall of evidence” which will stand even with several bricks knocked out
  - expert support: “I did ...”; “this shows that ...”

Consequences:

- Court time spent discussing the method, not the content
- Particularly difficult for proof to criminal standards
- Strong incentive to give up now ...

Eletronic evidence is ...

- ... easy to modify => easy to pollute
- ... to be found in many places – including other jurisdictions
- ... evanescent

BUT ALSO

- easy to copy (at least when digital)
- easy to search
- (fairly) easy to “secure” (hashes, WO media, cryptography, secure date-stamps)

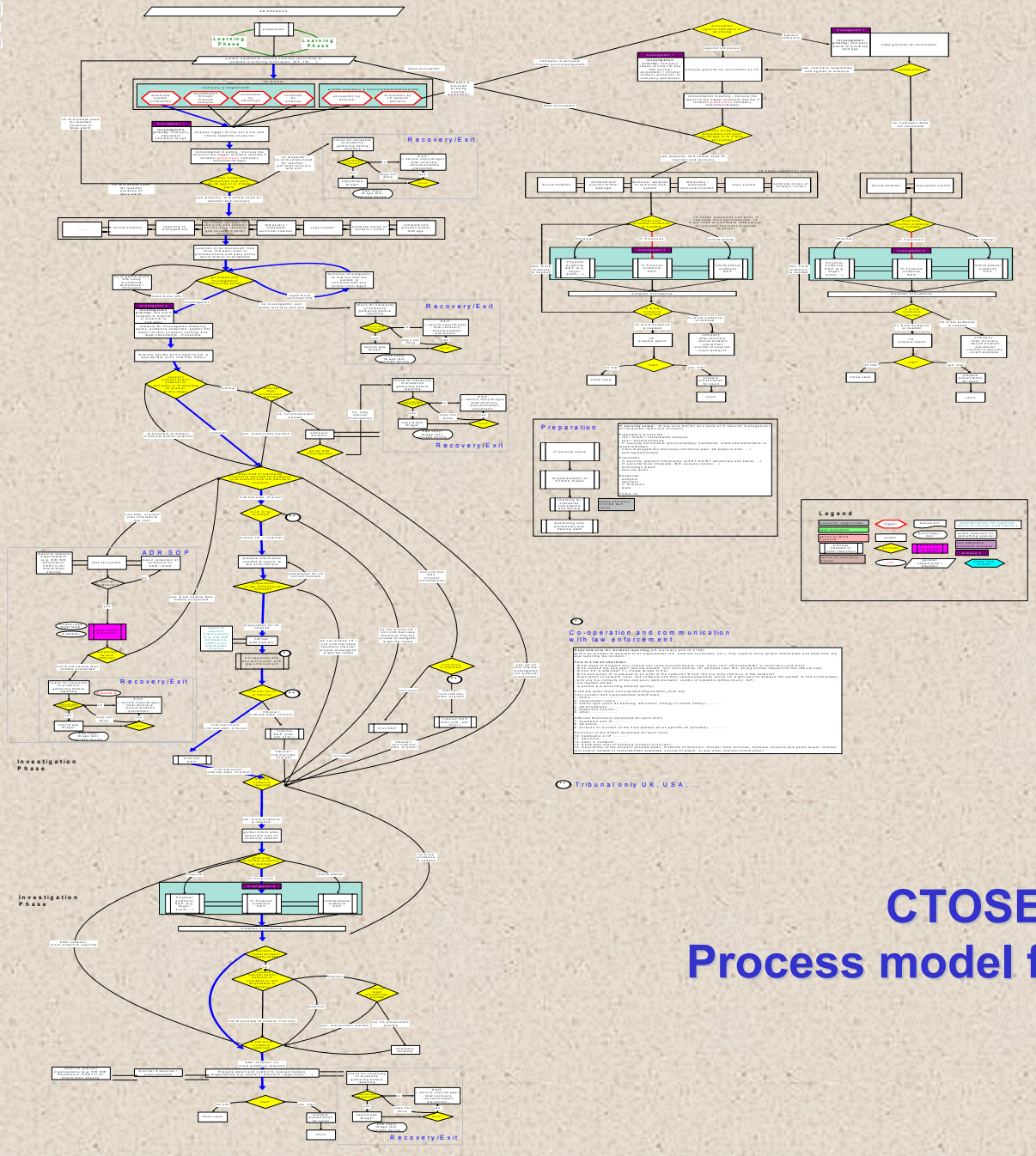
Handling evidence

- Established procedures: “chain of custody”
- How do we apply these to electronic evidence?
- What about what happened before?
- Mixture of electronic/physical evidence
- Admissibility/Weight of proof/Legality

Wouldn't it be nice ...

- ... if all investigators used the same approach, from sys admins. and IT security specialists right through to police
- ... if we could be sure that the same approach would be followed by investigators in other jurisdictions
- ... if the companies running e-services had systems running which could prove what was going on (pre-investigation)


ALCATEL
Cert-IST
QinetiQ
JRC
ipsc
CTOSE
I·A·T
Institut
Arbeitswissenschaft und
Technologiemanagement
Universität Stuttgart
Fraunhofer
Institut
Arbeitswirtschaft und
Organisation
University of St Andrews
ist



CTOSE
Process model flow chart

10 steps to Forensic Readiness

Identify potential sources & different types of available evidence.

Ensure monitoring is targeted.

Decide which crimes and disputes, electronic evidence may be required for.

Specify the circumstances when escalation to a full investigation is required.

Determine the evidence requirement

Train staff, to ensure all understand the legal consequences of incidents.

Establish a secure logging capability for the electronic evidence requirement.

Plan forensic procedures and adopt suitable internal/external standards.

Set up a policy for the secure storage and handling of logs.

Ensure that data are legally collected

CTOSE: what next?

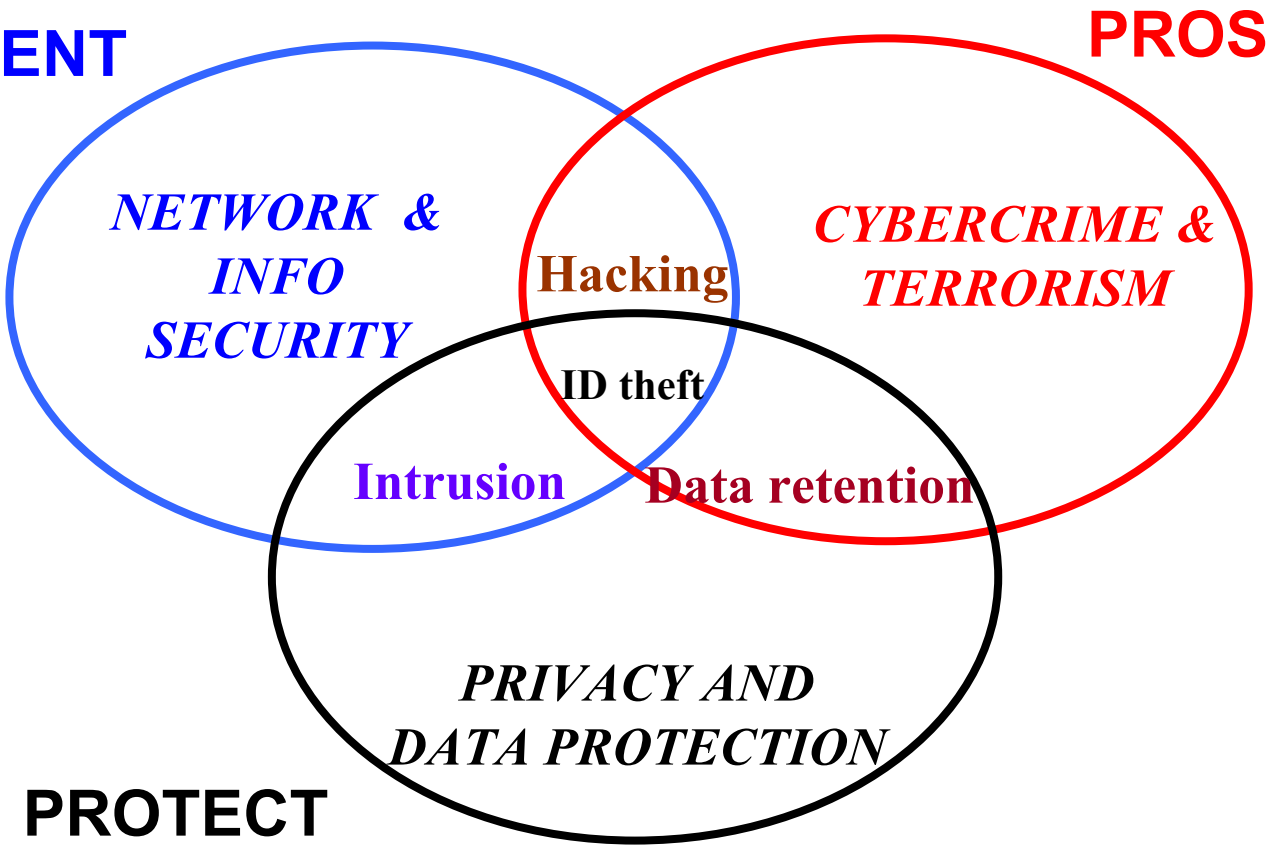
To build on, and develop further, the results of the CTOSE project, we propose to establish:

- A research network: ENDEM ("European Network for Digital Evidence Management")
- The CTOSE Foundation, in Europe, North America, and Australia

The wider context

- ICT more and more pervasive => new and larger-scale vulnerabilities
- More and more intelligence and autonomy are being built into the smallest-scale components
- Security issues in the e-world are international

Policy issues



ENISA: aims and tasks

- facilitating role (**not** a CERT/CSIRT)
- ensure high and effective level of security
- build on existing capability & resources
- develop expertise and stimulate co-operation
- assist in preparatory work for legislation
- principal tasks
  - collect information and analyse risks
  - provide advice
  - raise awareness

ENISA: structure (7/11/03)

- Established for 5 years
- Management Board: 1 rep. from each MS, 3 from the Commission, 3 non-voting members
- Executive Director
- Permanent Stakeholders Group

Outstanding policy issues

- Electronic signature
- Data protection in e-commerce
- Security culture and awareness
- Critical Infrastructure Protection
- e-identification/e-authentication
- Biometrics
- Digital rights management
- Crisis response