# Forensic Challenges for Handling Incidents and Crime in Cyberspace

**Barend Taute[1], Marthie Grobler[2], Simon Nare[2]**

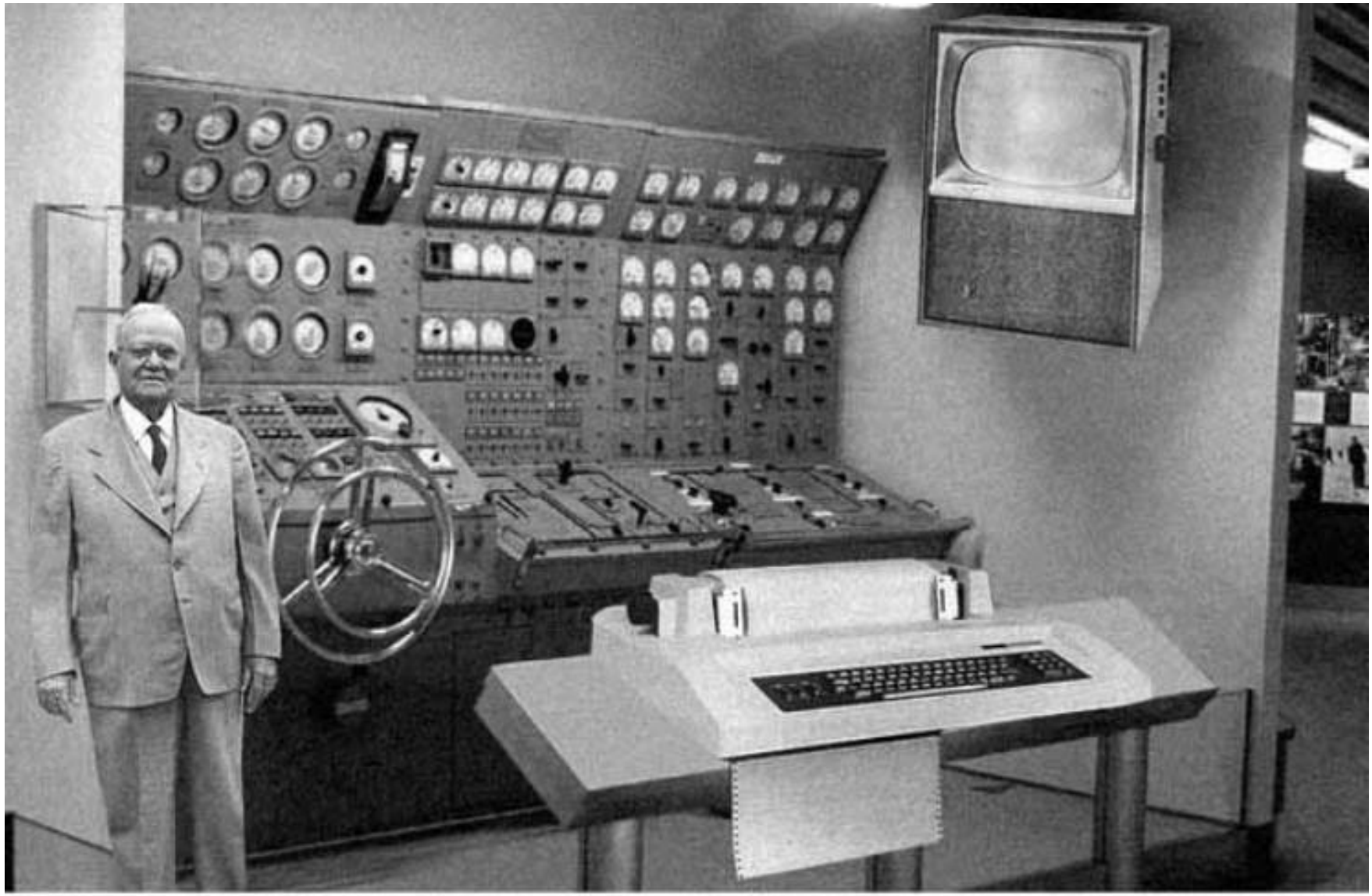
**CSIR Meraka[1], CSIR DPSS[2]**

# Contents

- Technology Challenges for dealing with Digital Forensics

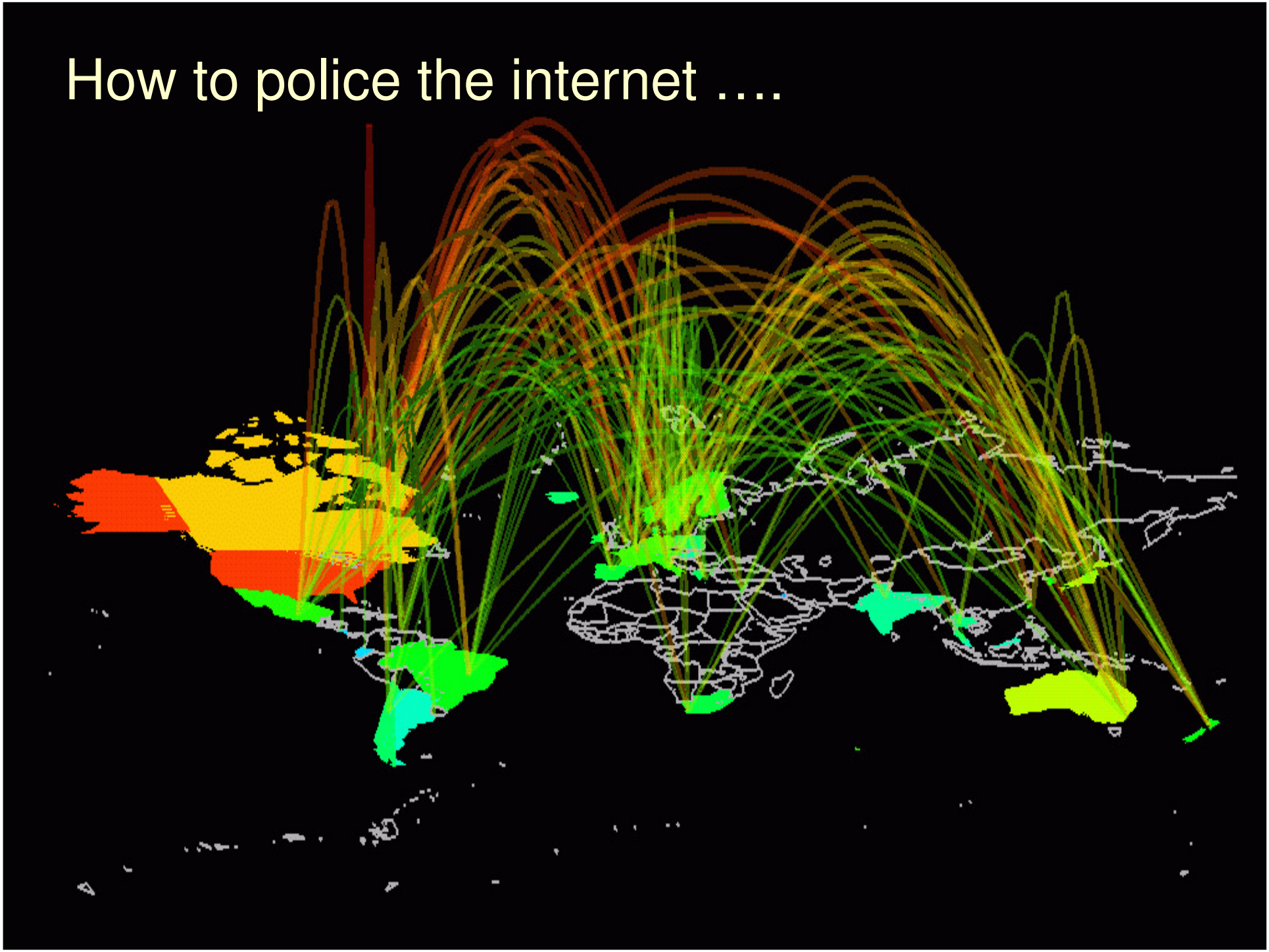
- The Time Factor in dealing with incidents and crime in cyberspace

# Model of the first home computer



*Scientists from the RAND Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 50 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use.*

# How to police the internet ….



# ICT is Important but Vulnerable

- The world is increasingly dependent on ICT for computing, communications, transactions, commerce, data storage, entertainment and a host of other functions.
- In a knowledge-based economy, information is currency and intellectual property, the fruit of knowledge work, is capital.

- The internet that forms the basis for global connectedness was built on an assumption of trust.
- This trust is violated by opportunistic hackers, malicious software, organised criminals and international terrorists to gain pride, money, power or information.
  - Impacting individuals, business, governments and countries
  - National Security and Commercial / Individual Security connected

- The battle for superiority rages between
  - ICT opportunities, speed and convenience
  - ICT threats, attacks and vulnerabilities




CSIR
our future through science

# *The Web Ushers In New Weapons of War and Terrorism*

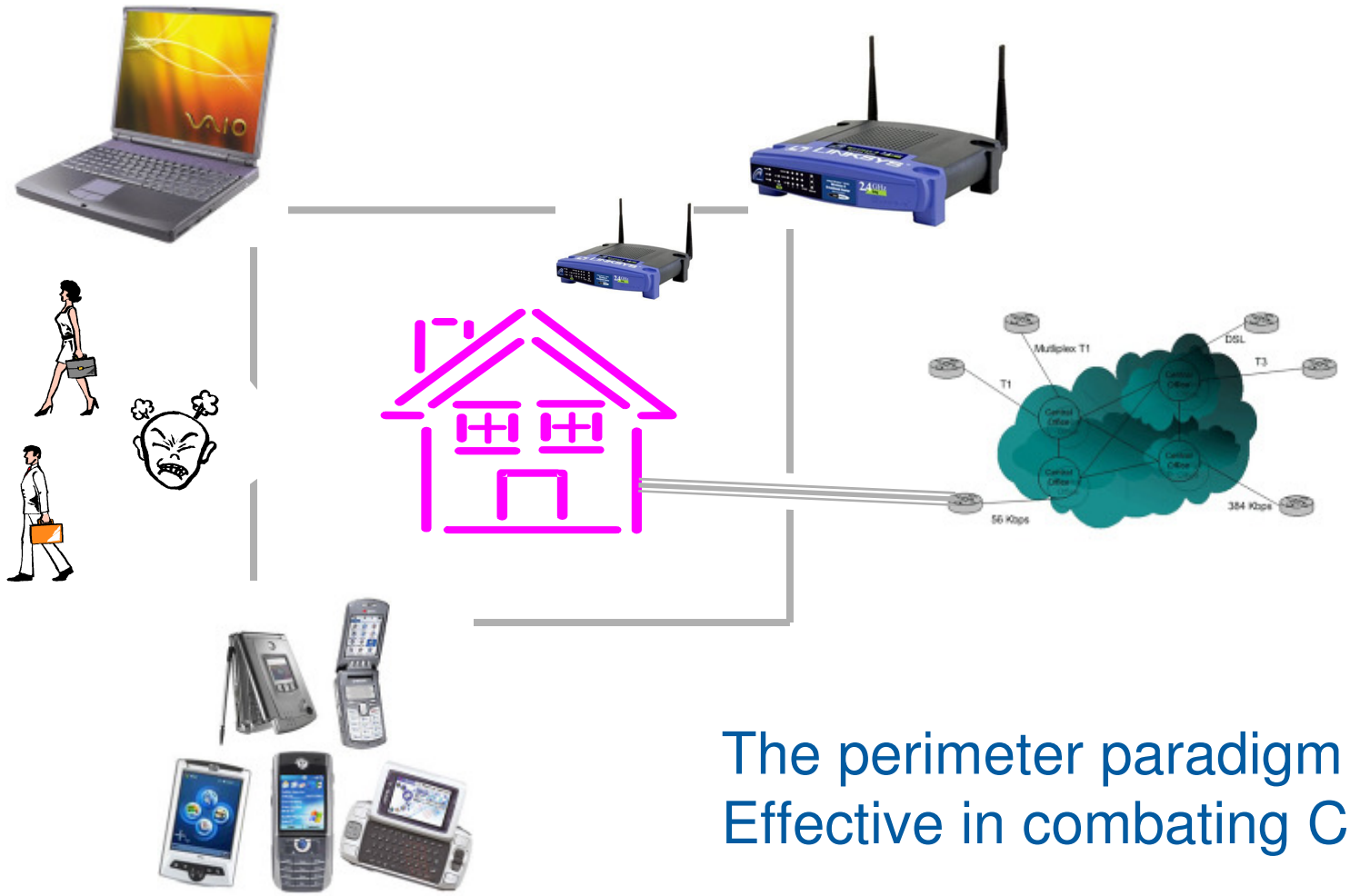
**Protesters, terrorists and warmongers have found the Internet to be a useful tool to achieve their goals. Who will bring law and order to cyberspace?**

- By Dorothy E. Denning
- Dorothy E. Denning
  Courtesy of the Naval Postgraduate School, Monterey, Calif




CSIR
our future through science

# The Perimeter Problem




The perimeter paradigm is not
Effective in combating CyberCrime

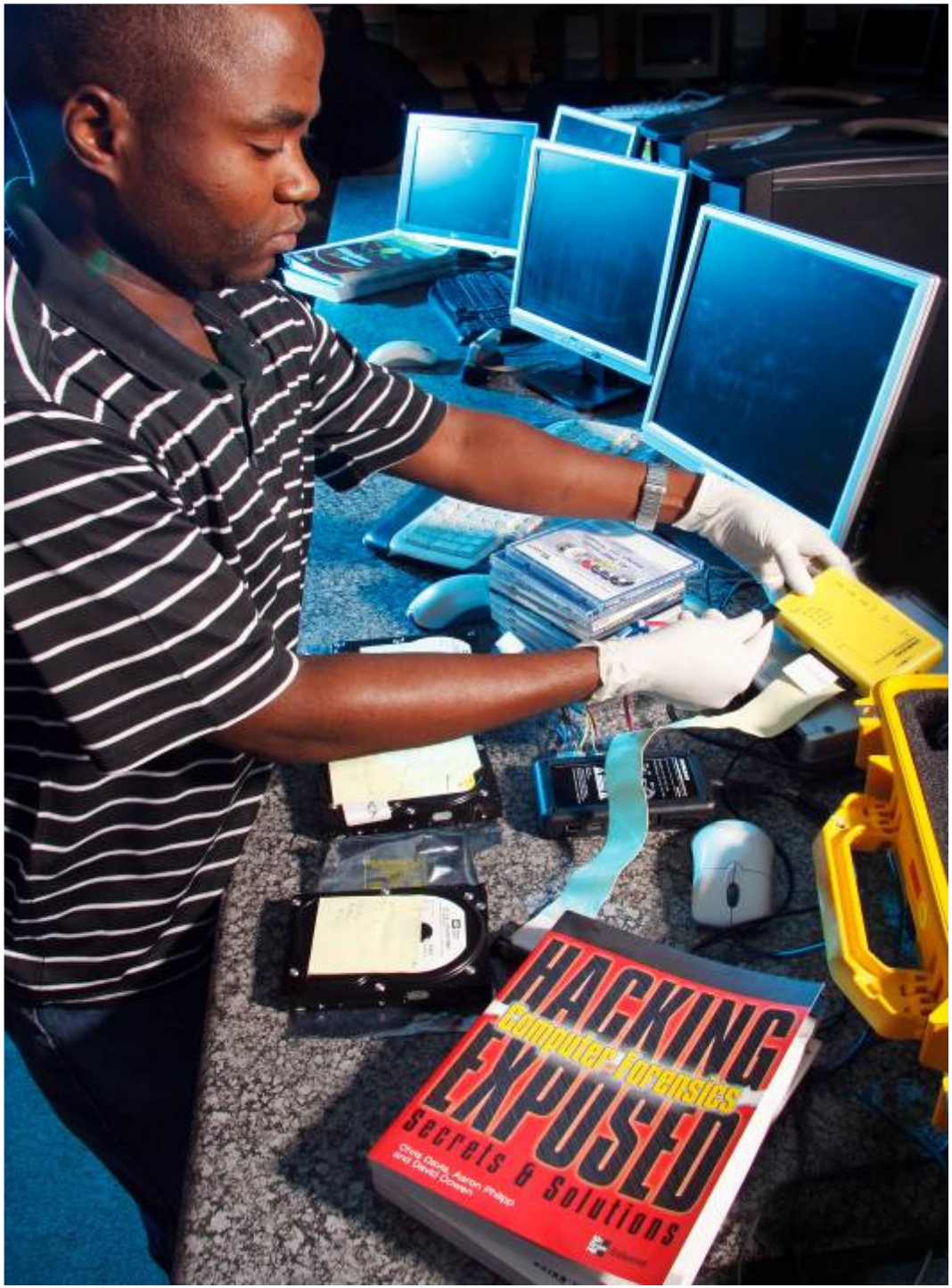



our future through science

# Typical threats and risks to information infrastructure

- Viruses and worms
- Trojans
- Botnets and Distributed Denial of Service (DDoS) attacks
- Vulnerability and exploits
- Spam
- Targeted attacks agains the systems

- *F-Secure in Finland says they receive about 15 000 potential malicious software alerts PER DAY, of which 1000 to 2000 are NEW ones. Then develop a "cure" and distribute to client base within about 1,5 hours.*




# Cyber Forensics

our future through science

# Different types of Digital Forensics

- **New technological developments pose new challenges to Digital Forensics**
  - **Dead Forensics** involves pulling the plug on a suspect machine or shutting down through normal administrative procedures; focus on static data but cannot address encryption.
  - **Live Forensics** is done on an actively running machine; considers the retention of volatile data and the expanded use of encryption; may modify data.
  - **Network Forensics** involves analysis of digital sources that are still actively processing and transmitting, that can impact system components; related to Live Forensics; the process uses a lot of bandwidth.
  - **Mobile Forensics** involves getting forensic information from handheld devices and SIM cards. Some of the data is stored at the service provider.

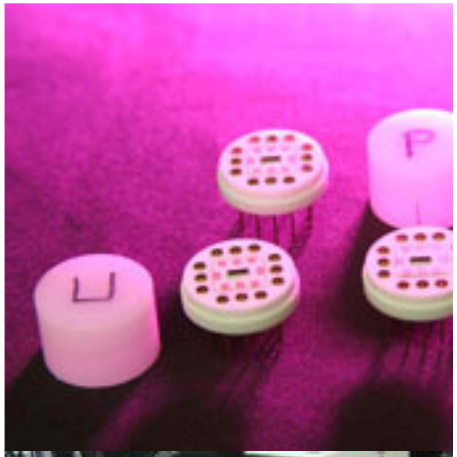
# Limited lifespan of media

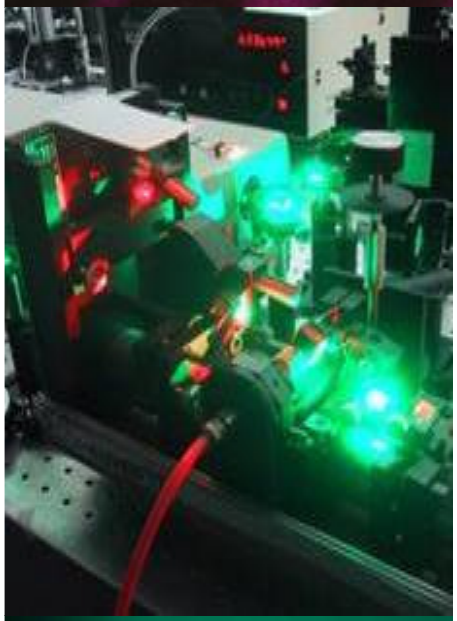
- Lifespan: until data loss due to irreversible degradation
- Widely different materials, conditions, handling
- Also depends on equipment to read / write
- Optical media has an optimal lifetime of 3 years, recorded life can be 50 – 100 years.
  - Ideal temperature range of 18 – 23°C,
  - Humidity range of 30 - 50 % (ISO 9660 compliance)
  - Higher temperatures may cause the disks to warp or crack.
  - Extensive exposure to UV light will accelerate the deterioration of the dyes used in optical media.
- Flash media has an optimal lifetime of 5 years
    - Memory stick, external HD, cameras, cellphones
  - Ideal temperature range of 5 – 70°C.
    range of 30 - 50 % (ISO 9660 compliance)





our future through science





# Limited lifespan of media (continued)

- Magnetic media
  - Life expectancy 10 – 20 years
    - Remember to archive playback systems
  - Ideal temperature range of 18 - 20°C.
  - Humidity range of 35 - 40% (higher humidity may cause mould growth).
  - Should never be stored in paper/cardboard - tend to generate dust that interferes with the media's functioning (use nonmagnetic immobile material, such as polypropylene).
  - Print-through occurs when tapes are stored for long periods without active usage.
  - Exposure to UV light exceeding 75µW/lumen will also hasten degradation.

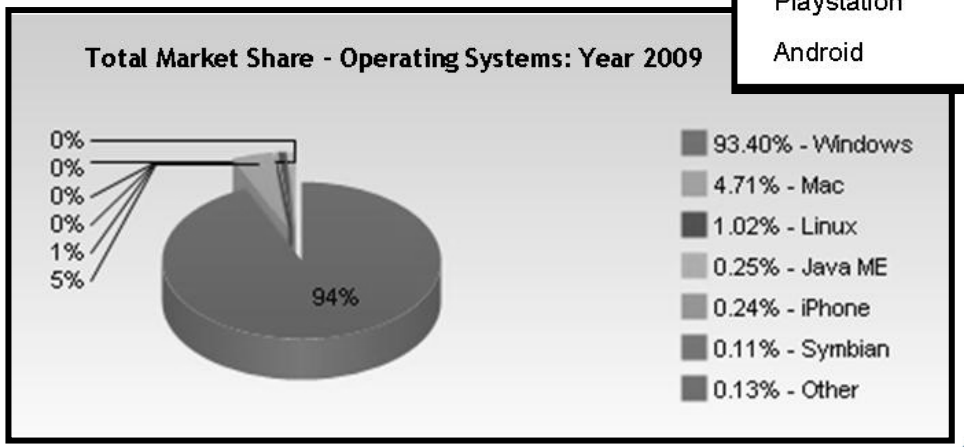



CSIR
our future through science

# Operating System distribution

- Operating System distribution and industry popularity has a strong influence on investigators' technical expertise

| Operating System | Total Market Share |
|---|---|
| Windows | 93.40% |
| Mac | 4.71% |
| Linux | 1.02% |
| Java ME | 0.25% |
| iPhone | 0.24% |
| Symbian | 0.11% |
| iPod Touch | 0.05% |
| Windows Mobile | 0.04% |
| Playstation | 0.03% |
| Android | 0.01% |







CSIR
our future through science

# Gaining access remotely

- A forensic agent is a tiny, covert software component that can be deployed by the network administrator using standard patch management systems.
- Similar to a rootkit, but legally acceptable (tested).
- Acts as receptor and transmitter for remote access to the system, in a forensically sound way.
- This agent should form part of the forensic readiness campaign of organisations.

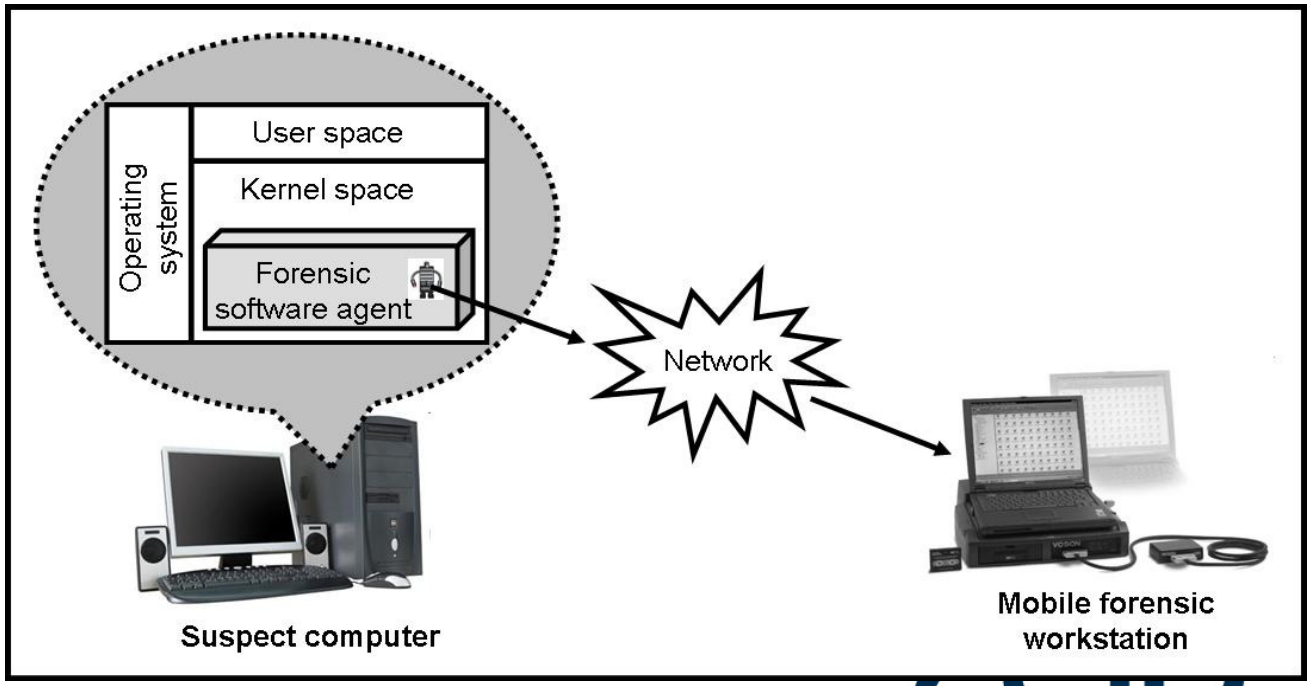
- Botnets use a similar technology




CSIR
our future through science

# Gaining access remotely (continued)

- Placed within the kernel space of the computer system, giving the forensic investigator administrative rights to the suspect machine.







CSIR
our future through science

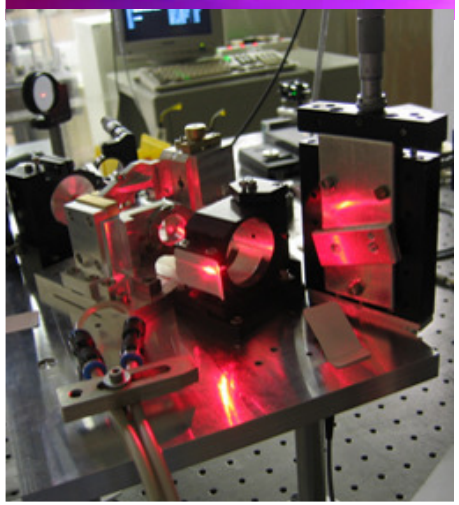
# Data modification during acquisition

- Images can slur

*a) Example image*

*b) Examples slurred image*

- Forensic investigators can potentially modify the evidence
- Criminals use anti-forensic programmes *eg hide, regular updates during live acquisition, cryptography*



# Demonstrating authenticity

- Electronic evidence still needs to meet the same legal criteria as traditional evidence.
- These criteria require evidence to:
  - be relevant to the issue at hand;
    - Limits to “accidental evidence?”
  - be authentic (the evidence is what it purports to be);
  - not be unfairly prejudicial to either party in relation to the evidence’s probative value; and
  - not be hearsay or if hearsay, able to meet the requirements for an exception; be the original or duplicate of the evidence or able to meet an exception to that rule.




CSIR
our future through science

# Ensuring court acceptance

- Court systems slow to accept new technology
  - *"While judges may resist the use of technological advances within the court itself, we cannot avoid the impact of these scientific and information revolutions on the substance of what we do. The rush of new scientific developments has been so swift that the court system is struggling to deal with the expert testimony they produce…"* (Shelton 2006).

- According to studies done by Jones and Fox, between 85% and 95% of 18 to 30-year olds are online, whilst only 50% of 50-year olds and older are online.
- Prolonged process to ensure court acceptance of technology.




CSIR
our future through science

# Lack of standardised procedures

- Every country has own rules
- Leads to uncertainties about the effectiveness of current investigation techniques.
  - ISO 27037 is working on international guidelines for identification, collection and / or acquisition and preservation of digital evidence
    - 2011 is planned publication date
- Leads to suboptimal use of resources
  - investigators gather worthless data that take unnecessary time
  - this data have to be stored and take up valuable space.



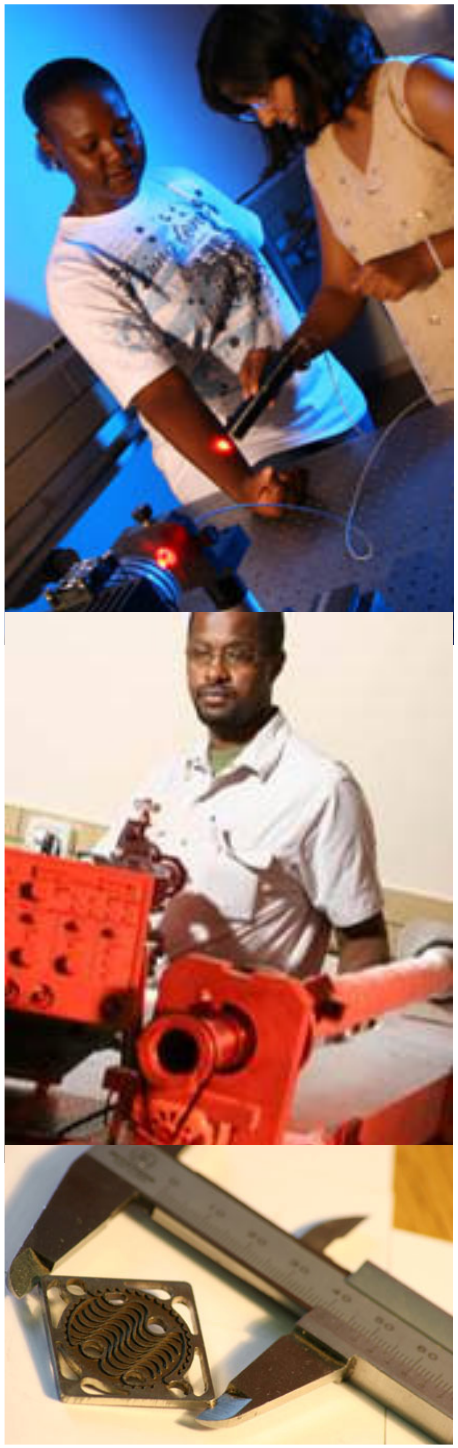

CSIR
our future through science

# Cryptography and Redundant Array of Independent Disks (RAID)

- Cryptography and RAID can render a forensic image useless
  - Users can only decrypt an encrypted drive with a unique password.
  - Data retrieved from different disks of a RAID system need to be puzzled together before it can be considered as evidence.
  - During a Live Forensic Acquisition, the *data is read directly from RAID in the normal manner,* without the need to puzzle the data together before it can be considered as evidence.




CSIR
our future through science

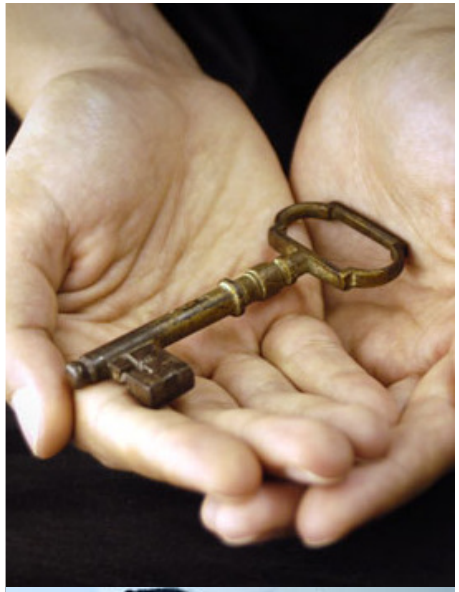


# Trojan defence

- Owners of suspect systems claim that a third party hacked into their system and committed some offence as if from their computer, i.e. a hidden Trojan on their system.
- With Dead Forensics, forensic investigators may be able to find traces of a Trojan on the suspect system, but it is not always possible to prove whether this Trojan was active and could have enabled the offence from a remote location.
- With Live Forensics, investigators can retrieve the suspect system's pagefile. This file will indicate whether a Trojan embedded in the system is active or not, and is facilitating a third party to commit an offence remotely.




CSIR
our future through science



# Limited window of opportunity

- Relates to time factor
- Live Forensic Acquisition can only be performed if the suspect machine is in an active session. The suspect machine needs to be logged on for the forensic investigator to gain access to it.

# Bandwidth restrictions

- Bandwidth restrictions can limit/slow down acquisition process
  - Since the suspect machine is live and active, forensic investigators need to connect to the **forensic agent** installed on the machine via a network.
  - Copying data as digital evidence from the suspect machine to the forensic workstation will slow down the bandwidth, especially if there are a large number of other computer users also using the bandwidth at that time.
  - In addition, large remote acquisitions may have to be done after hours to accommodate the small South African bandwidth capacity.




CSIR
our future through science

# Differences between Cellphone and Computer Forensics

- **Computer Forensics:** – Only a Few Major Operating System Standards: Windows, Mac, Linux. Standard practice is to image the Hard drive and Examine Data.
- **Cellphone Forensics:** – Multiple Operating Systems. Various Communication Standards. Each manufacturer has their own OS: Nokia, Samsung, Motorola, Palm, Blackberry, Apple, etc., etc. Communication Standards Evolving. Connection/Cable challenge.
- **Mobility Aspect:** - Phones are live things roaming around. It's not just about what's on the device, but where has it been?
- **For the examiner,** the job is harder, as each system is unique and proprietary. Always a moving target, as the manufacturers are changing systems regularly. Evolving Network Technologies require new methods of extractions. We're at Windows 95 (probably) compared to computers.

# There Is No One Size Fits All Solution

- Forensic process:
  - Collection – Examination – Analysis – Reporting.

- A Number of Mobile Device Forensic Tools on the Market
  - X-ray, Paraben, Oxygen, Cellbrite, …
  - Some don't support the full forensic process.
- Each Have Their Strengths and Weaknesses. Plenty of overlap of support for devices, but Success with Devices varies

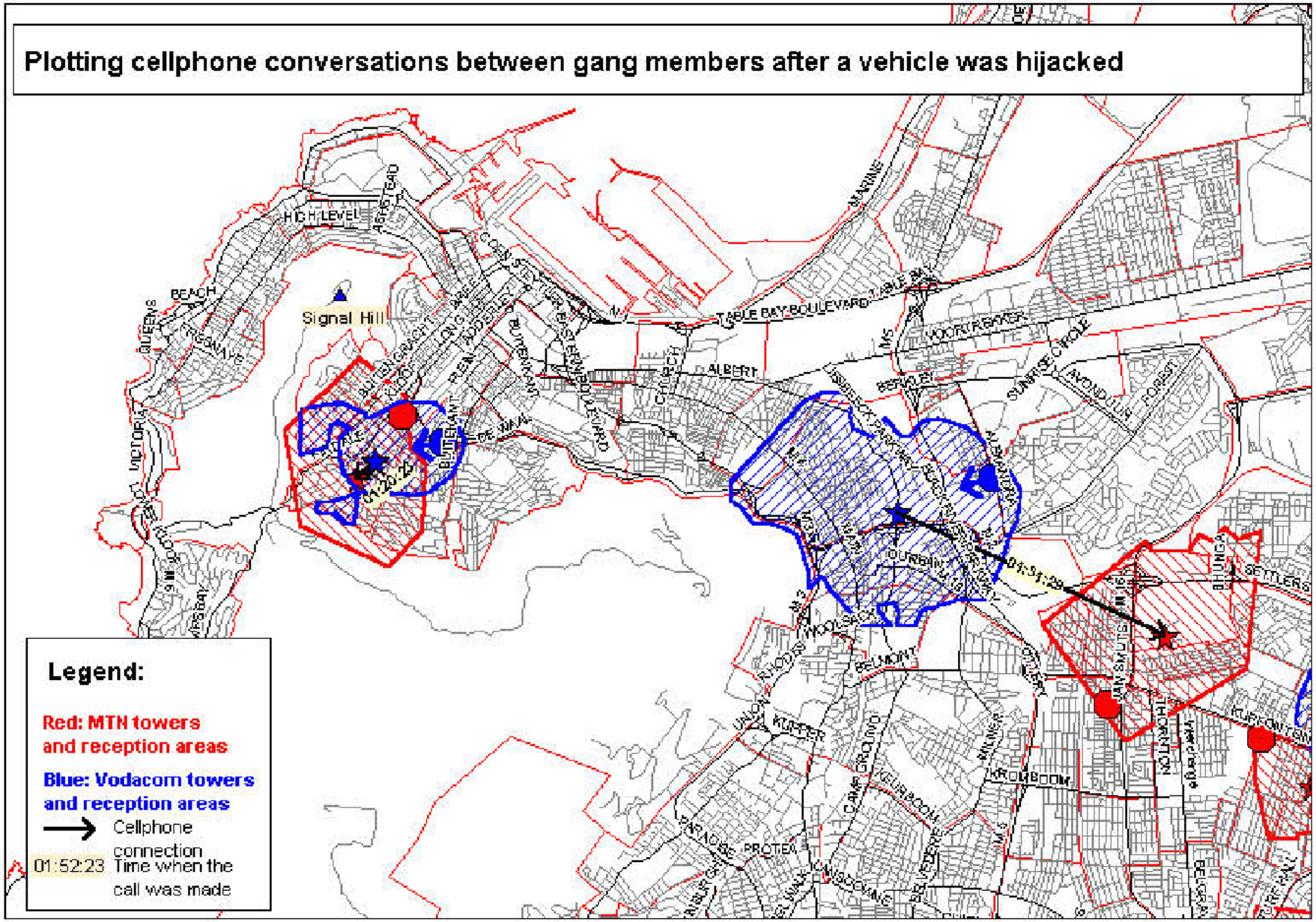

**Paraben**

- This is due to the challenges in supporting the continuous introductions of new phones and changing technologies. It's a tough job for the examiner to keep up – And equally difficult for the companies making the tools.
- Examiners Never Know What They Are Going To Get! Often need more than one tool.




CSIR
our future through science

# Plotting cellphone conversations between gang members after a vehicle was hijacked



# Information Security

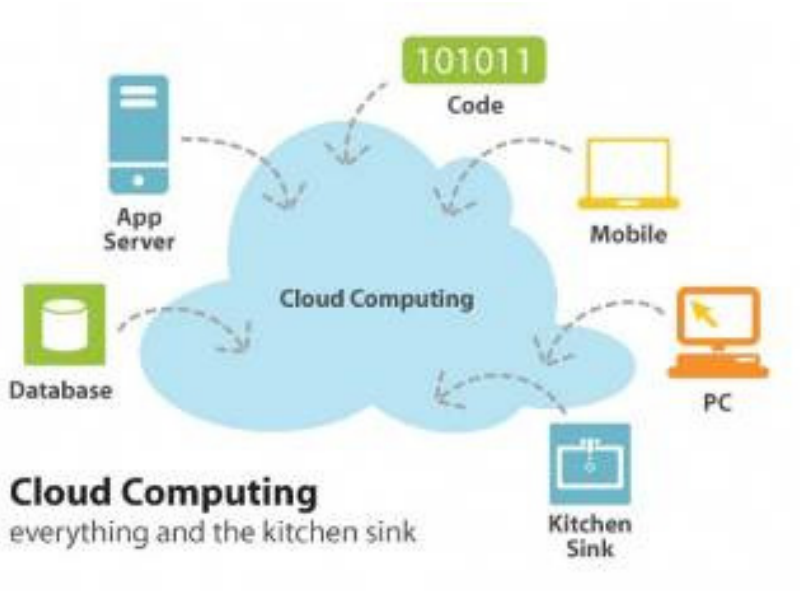
**“Information Security”** / **“cyber security”** is

an all-encompassing concept for building confidence in the use of information and communication technologies (ICT) through increased

confidentiality, integrity and availability
of the information and the information systems.

# Global connectedness

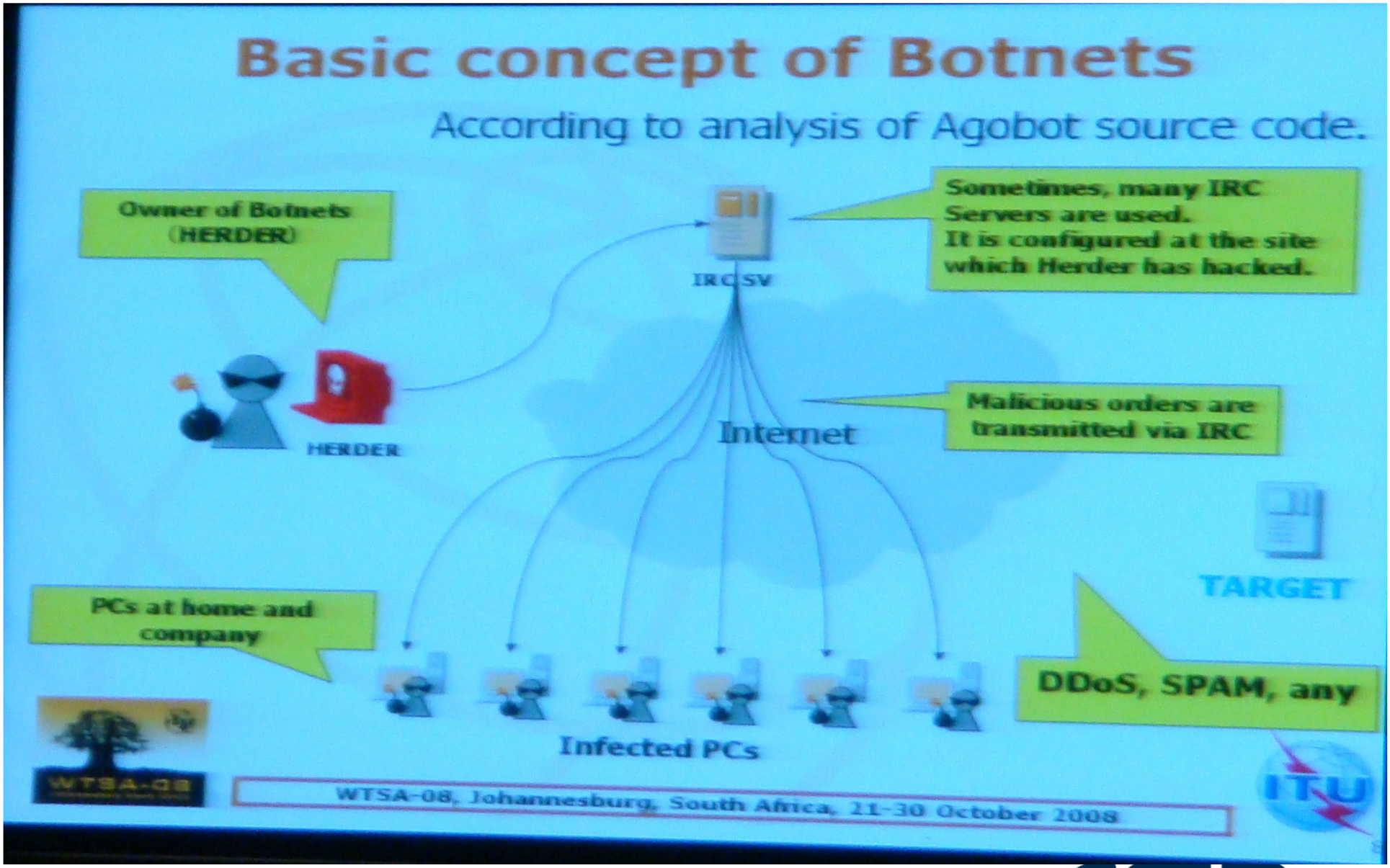
- Threats and attacks in cyberspace
- Incident response – try to stop the security breach that happened to minimise the damage
  - Not much concerned with WHO, just want to stop
- Forensic process will try to substantiate guilt
- Optimal process will include a forensic chain of evidence while the incident is stopped
- However, a lot of incriminating intelligence may still be gathered

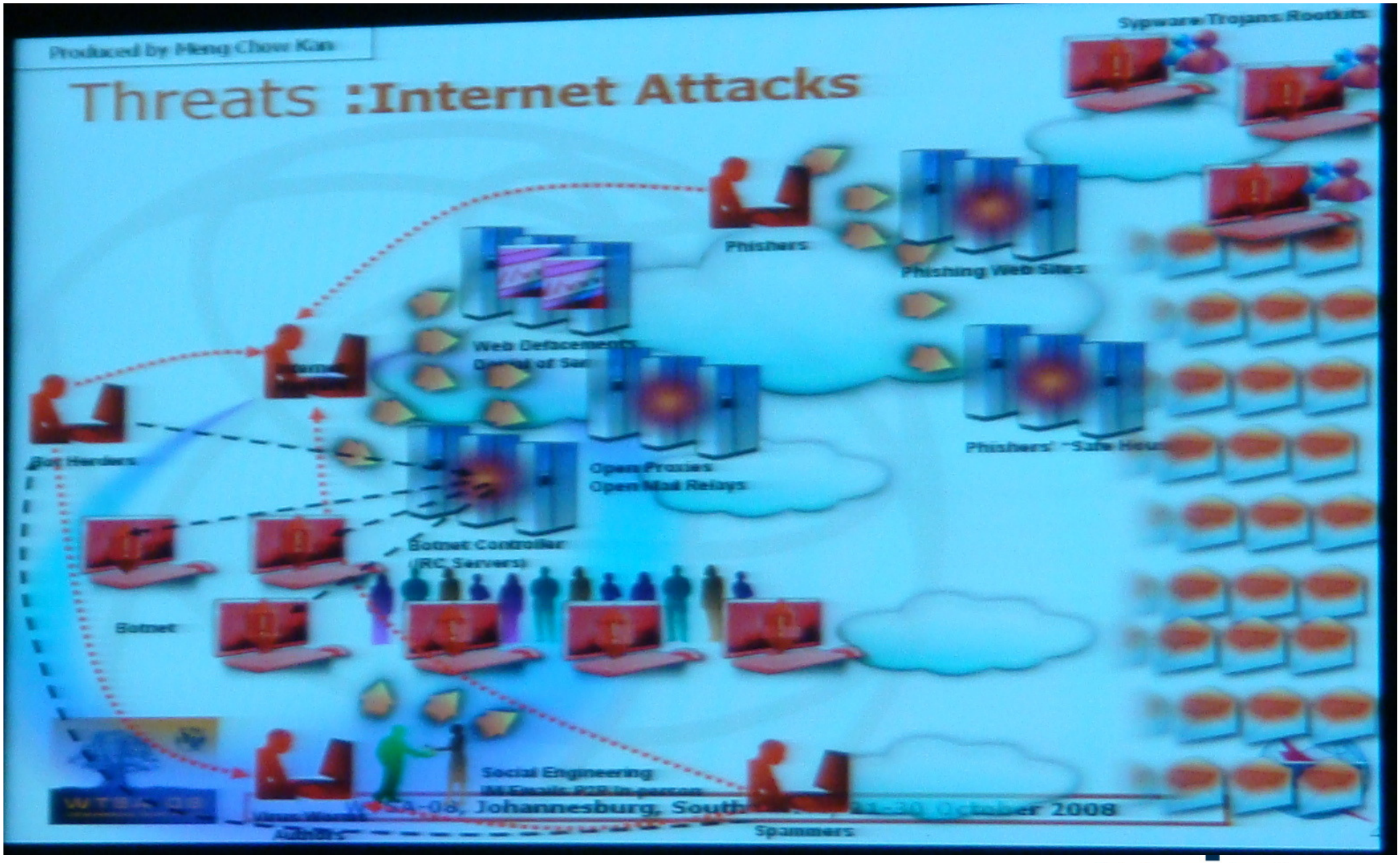






our future through science










our future through science

# The time factor in dealing with incidents and crime in the cyberspace

- Often not enough time to call the police when a cyber incident is in progress.
  - Incident = security breach
- Cyber Forensics First Responders arrive first at the crime scene and can handle at least 80% of cases correctly.
- The law requires that people gathering evidence be qualified to do so or be authorised (trained, appointed)
  - What about ICT staff? Is the law clear?
- Some companies do not have qualified staff within their response team – but they may be able to stop an incident.
- Wrongly collected data may not be used for evidence
- Forensic  analysis of a live incident has some technical challenges
  - modified data, changing websites (can't replicate)
  - Custodian of the evidence may not be clear (moving, changing)
  - Not simple to follow the procedures of Forensic soundness to maintain the evidentiary chain on live incidents like hacking or malicious activity by a botnet
    - by the time you try to collect evidence, things have changed.
- Evidence on live transactions require bank cooperation

# Role of a Computer Security Incident Response Team (CSIRT)

- CSIRT = A computer security incident response team is a dedicated team of information security specialists that prepares for and responds to IT security breaches and incidents.

- How CSIRTs operate:

  - Global networks, common interest in protecting the internet
  - Relationships and trust through regular interaction
  - Speed of reaction far outstrip legal process for legitimate requests

- Immediate response to safeguard the internet
- Followed by support to forensic processes where necessary – eg to identify a culprit
- ECT Act has limitations wrt to a cyber criminal outside the RSA jurisdiction.

# The Information Security Centre of Competence

**Funded by the Dept Science and Technology**

**Coordination Hub at the CSIR Meraka**

**<u>Main Purpose:</u>**

**Increase INNOVATION in Information Security in South Africa**

# Innovation Missions

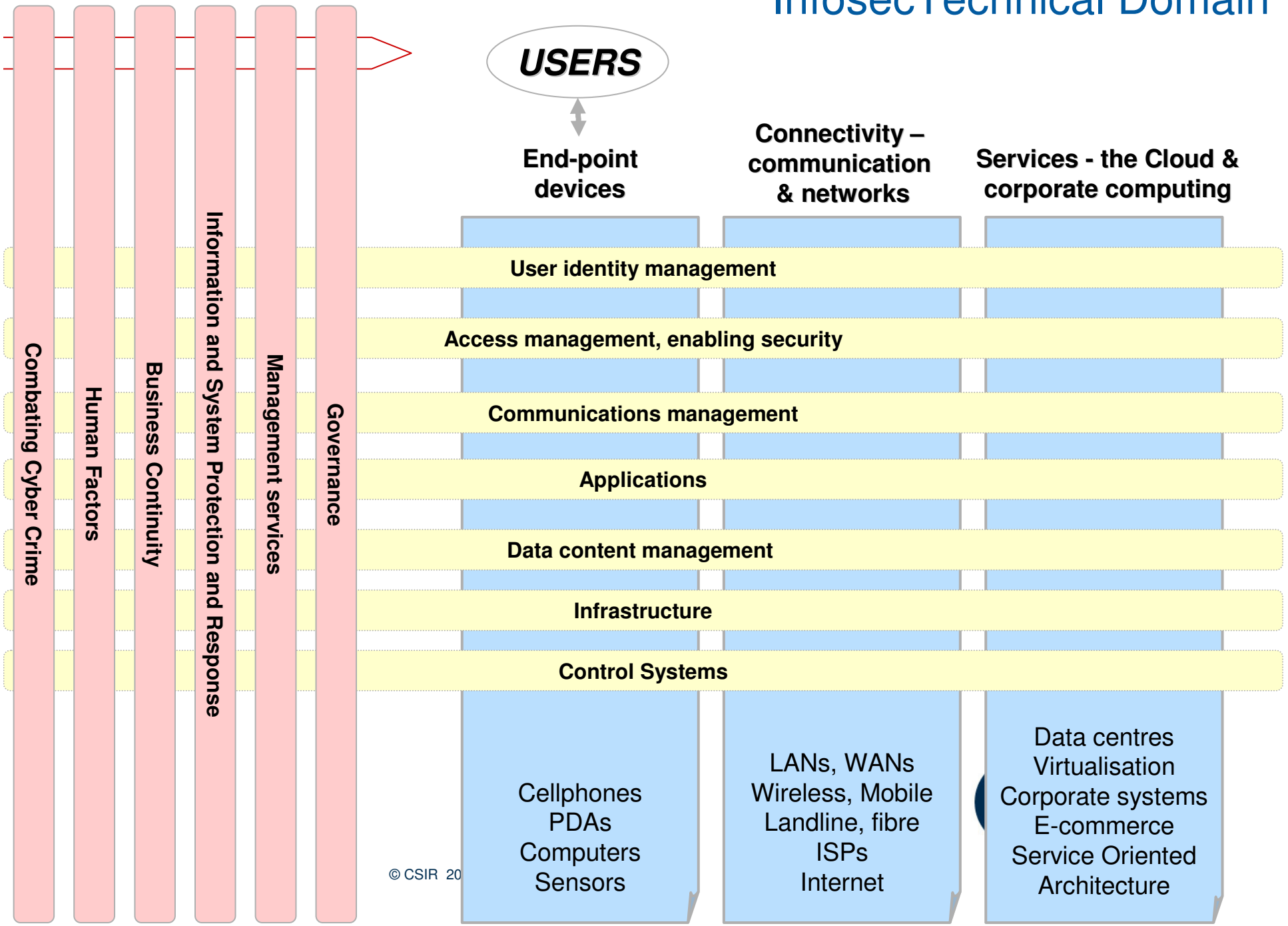
- Creating an Information Security Innovation Environment
  - Understand and mobilise the NSI, national Research Agenda, access to international knowledge, build human capacity, facilitate the innovation process

- Market Mission A: Innovative Products, Processes, Services and Institutions to mitigate Cyber Security risks
  - Crime investigation, incident response, critical infrastructure, information warfare

- Market Mission B: Innovations to enable eSecurity in Government
  - Public information, ICT operations, compliance, eGovernment products and services, security and privacy

- Market Mission C: Facilitate commercialisation of niche, high-value, globally competitive, Infosec Products & Services
  - Competitive opportunity or market failure opportunity

# InfosecTechnical Domain



# ISCoC – opportunities for cooperation

- Cyber Security / Crime / Risk Mitigation
  - Law enforcement and forensics
  - Incident response
  - Awareness, training
  - Crime investigation tools
- eSecure Government
  - Standards, guidelines, processes, compliance, governance
  - eGovernment products and services
  - Identification as a key, underlying requirement
  - No eGovernment if there is not SECURE eGovernment




CSIR
our future through science

# Concluding Remarks

- Technology challenges to digital forensics
  - The domain is dynamic and complex
  - New technologies develop much faster than forensic solutions to deal with them
  - Ongoing research and development, and training of experts are crucial
  - LE to do forensics at a level that keeps up with technology
  - Key legal challenge is with the international jurisdiction of forensic evidence
  - The global nature of internet means some forensic evidence can only be collected with cooperation from LE or interpol in foreign countries. Solving international cyber crimes require good relationships with LE in foreign countries.

- Time factors in dealing with incidents and crime in cyberspace
  - Some incidents are so severe and urgent that stopping them overrides the requirements of a sound forensic process for criminal prosecution
  - CSIRTs operate faster than any legal process

- ISCoC – invitation to identify needs for innovation
  - Information & communication technologies and the law

# Questions / Suggestions ?