Cooperation EU-South Africa in security research

Michel Riguidel, Telecom Paris-Tech
michel.riguidel@telecom-paristech.fr

[1]

My presentation agenda

✓ **Outline the research topics identified at the recent BIC EU – South Africa cooperation workshop on ICT trust and Security held in August 2011**

1. Trust Management for techno-socio-business ecosystems for emerging economies
2. International Cyber security research
3. Financial Infrastructure Protection
4. Enhanced cooperation with Law Enforcement approaches to deal with cybercrime
5. Coordinated approach to cross domain multi-disciplinary research in the "Future Internet"

Topic of cooperation identified already

- **Trust Management for techno-socio-business ecosystems for emerging economies**
  - Challenge: the need for collaborative on-line and real-time trading environment
    - large enterprises (LEs) such as suppliers and financial institutions transact with Very Small Enterprises (VSEs)
    - lack of ICT infrastructure, VSEs dependent on mobile communications
  - Solution: requires development of an "indigenous trust model", a model that reflects the unique requirements of emerging economies
    - experience a sense of normality in social controls
    - involve community and community leaders (e.g. as trust moderators)

BIC

BUILDING International Cooperation
for Trustworthy ICT

European Commission
Information Society and Media

[3]

Topic of cooperation identified already

- **International Cyber security research** (½)
  - The challenge: could Africa become the home of the world's largest botnet / cyber security pandemic?
    - the fast pace of increased broadband (and largely wireless) internet penetration
    - high levels of computer illiteracy, sometimes ineffective legislation
    - anti-virus software may be un-affordable or too technically sophisticated for the low-cost devices that are still used
    - heterogeneous continent harbours a large socio-techno digital divide that needs to be accounted for in developed security solutions

[4]

Topic of cooperation identified already

- **International Cyber security research** (2/2)
  - Solution: International, collaborative research can address these challenges by looking at a variety of approaches that require innovative implementation, including:
    - ISPs taking a bigger role / responsibility with the provision of security services so that much less depends critically on the end user
      - i.e. creating "thin clients" vs the "thick client" where the ISP only provides the pipeline
    - Bottom-up, community oriented approaches to Critical Information Infrastructure Protection
    - Sector based cyber security alliances (universities, industries, banks) that share information / best practice
    - Opening up international data-exchange architectures for cyber security
    - Models and platforms for national and regional cybersecurity coordination (citizens, industry, security sector, government, regional governments)

[5]

Topic of cooperation identified already

- **Financial Infrastructure Protection**

    - Challenge: a need for providing secure eBanking in the face of a barrage of sophisticated, creative, efficient and persistent phishing attacks
        - The banks are providing competitive eBanking services for computers and mobile devices, which are highly subject to these threats
        - The current approach is to have individual approaches to deal with this but there is a need to collaborate together and view reducing and fighting crime as a shared and non-competitive responsibility

Topic of cooperation identified already

- **Financial Infrastructure Protection**

    - Solution: public-private-partnerships including the current close cooperation with the Police as well as local and international research collaboration on issue such as:
        - Mathematic analysis of normal vs abnormal patterns in banking behaviour.
        - Packaging abnormal behaviour (suspicious behaviour, attack vectors)
        - Anonymising the shared data and information to effectively address concerns about reputation loss, paramount client privacy and anti-competition laws
        - Establishing a Financial Sector Computer Security Incident Response Team (CSIRT) that meets international standards for reducing risk and responding to incidents. SA has already had collaboration with ENISA, EU CSIRTs, USA and others
        - Leveraging technical developments in the mobile and cellular networks to provide increased trust as well as usability of eBanking solutions

Topic of cooperation identified already

- **Enhanced cooperation with Law Enforcement approaches to deal with cybercrime**

  - Challenge: to deal with a variety of cyber crimes with significant criminal intent
    - increasingly sophisticated social engineering
    - customised Trojans and commercial spyware, computers and information for sale
    - "ransomware" (the next level "scareware")
    - attacks on mobile devices and even signs of attacks on automobile computer systems
    - there are strong signs of this being organised cyber crime with the criminals operating directly or by proxy from just about anywhere in the world

Topic of cooperation identified already

- **Enhanced cooperation with Law Enforcement approaches to deal with cybercrime**
  - Solution: In South Africa, this is already addressed through closely intertwined and good relations between law enforcement and technology providers e.g. ISPs on a national basis, adopting a mutually supportive strategy.
    - Impact business model by capturing and justly punishing of the cybercriminal.
    - Deal with the enforcement (sentencing gap between physical crime vs cybercrime)
    - International, collaborative research (including technology-policy-legislation strategy) should give direction to the serious challenges with the prevention/combating, investigation and prosecution of cross border cyber crime
    - Prioritisation needed on better coordination of the country's cross border cyber crime detection and prevention.
      - How can this effectively be elevated to the highest authority? What is the national "business case" for increased attention, coordination and funding?

Topic of cooperation identified already

- **Coordinated approach to cross domain multi-disciplinary research in the "Future Internet"**
  - Challenge: South Africa does not currently have an active debate regarding coordinating all of the research aspects of the Future Internet, as is the case in Europe and elsewhere.
    - This crucial debate is shaping the creation of the next generation of the Internet with an increase of Internet based services.
    - The physical and virtual worlds are converging. There is a revolution in data networks such as LTE.
    - Open delivery platforms are becoming the norm.
    - While the developing world including South Africa is catching up and mobilising the current Internet, and wrestling with the trust, security and privacy issues that it brings, it also needs to be ready for the Future Internet.
    - This is as true for governments as it is for industry, and it is clear that any Future Internet will require significant public-private-partnerships