Cybersecurity and Africa

Benoît MOREL
Carnegie Mellon University
Afrinic
Cyberization of Africa

• The new big development in the cyberworld
  – 6.8% penetration population today
  – …but the growth is **phenomenal**

• Changes the digital divide

• Revolutionizes the economy and social structure of African countries

• But this is at a time when cyberspace has become a very dangerous place
Need for quick progress in cybersecurity

• Protecting government secrets (agent.btz) and messages (ghostnet)
• Protecting financial information (silentbanker)
• With high capacity connection: haven for botnets (Conficker) and other forms of infections
• Critical infra-structures (of tomorrow?) and the cyber-protection of scada (Supervisory Control and Data Acquisition)

• Need for “National CERTs” (Computer Emergency Response Team)
Challenges

• No template in US or Europe
  – (in fact their governments are not good examples to follow: too dependent on private security industry. No government is a leader in cybersecurity. Cybercriminals outsmart them)

• Where to get the expertise:
  – No centralized repository of knowledge and expertise
  – Needs are specific:
    • what kind of training?
    • how large an operation a national CERT should it be?
    • Can it generate revenue live on its own or should it be a government agency?

• Economics:
  – Cost of training, security tools
  – what to invest in, how much, what return on investment?
Some Answers

• Building a national CERT is a protracted process.
  – Not a case of one size fits all: countries are different
  – Needs are evolving,
  – a lot of learning by doing,
  – cooperation among CERTs. (crisis management, national points of contact, keeping abreast)
  – Forum for Incident Response Teams (FIRST):
    • a “club” to which any CERT must belong (or at least seek to belong as a form of accreditation).

• Tunisian example:
  – Only African CERT in FIRST
  – 6 years of experience,
  – experts in open source/free tools
  – Prepared to share their knowledge

• In the US:
  – Carnegie Mellon has a lot of expertise and can be a precious interface between African countries and the rest of the US
  – National Defense university
National Defense University

• 20 years of experience in training in cybersecurity taught them that:
  – Cybersecurity is not only about computers, it is also (mostly?) about information.
  – Their 14 weeks curriculum reflects that.
• Originally designed for US government,
  – opened to foreign nationals
• They want to open to Africa
• Costs are limited as no money can come directly to them
  – (this has to go through the “local” US embassy)
• They also go to foreign countries for specific trainings:
  – (Examples: Romania, Sweden, Singapore, Japan)
Smart phones

• Potentially the most pervasive device.
  – Worldwide, but especially in Africa
• Already a target for variety of attacks
  – (data, communication, etc…)
• Bound to become a a very challenging cybersecurity concern
  – More processing power than previous computers, but less than existing computers.
  – Make them intrinsically vulnerable
The Future belongs to Africa

• That begins with the Africans ensuring that they reap the full benefits of the IT revolution, i.e. taking cybersecurity seriously and building national CERTs

• We think we have something to offer fitting the African needs in cybersecurity

• We want to be part of the future of Africa

• Hence we want help build it

• My email: bm1v@andrew.cmu.edu