Watch, Warning, Incident Response (and Other) Capabilities

Sy Goodman
Georgia Tech
ITU West Africa Workshop
Cape Verde, 27-29 November 2007

Crime, Security, Assurance

- Cyber Crime (deter, detect, investigate, apprehend, punish)
- Cyber Security (vulnerabilities, threats, and what to do about them)
- Information Assurance/Trust (confidentiality, integrity, access; systems do what they are supposed to do, and not do anything else)

ITU High Level Expert Group
Work Areas

- Legal Measures
- Technical and Procedural Measures
- Organizational Structures
- Capacity Building
- International Cooperation

Operational Functional Capabilities

(assuming you already have laws, national policies)

- Prevention and deterrence
- Watch and warning
- Incident management (includes forensics)
- Consequence management (includes forensics)
- Standards, certification, compliance
- Education/culture/professional defenders

Where might these functional capabilities reside in small developing countries?

- CERTs – Computer Emergency Response Teams
- CSIRTs – Computer Security Incident Response Teams

("Response Teams" sound a lot like fire departments or SWAT teams)

- National Cyber Security Centers

National Cyber Security Centers

- Really should be concerned with more than just cyberspace in the form of the Internet
- Why a national (government) center?
  - Best use of very limited human resources
  - Perhaps the only place that could take on a broad range of the operational functional capabilities, especially if they are to include law enforcement
  - Private sector too weak, and there is little or no business incentive
  - Government ICT assets a major part of what needs protection (e.g., e-government, TLD)

Institutional Home for NCSC?

- An independent organization within a Ministry
- As a department in an existing center (e.g., a National Computer Center)
- As a unit under the national telecommunications regulatory agency
- As a unit outsourced to the private sector (domestic or foreign)

Other Considerations for an NCSC

- Functions and constraints must be defined by law. Potential for abuse. Would need oversight. National security? critical infrastructure protection? public safety?
- Specification of who is to be helped (government, all citizens).
- Operational agency for international cooperation

NCSC in Africa

- So far, we have only been able to identify two CERT/CSIRT organizations (please tell us if there are others that would qualify as functioning NCSCs!!)
  - Algeria (may not be functioning well)
  - Tunisia (and we turn to them now)