

Community-oriented Computer Security Incident Response Teams (C-CSIRTs)

David Ellefsen and Basie von Solms
iellefsen@uj.ac.za | basievs@uj.ac.za
Academy for Information Technology
University of Johannesburg
ZACON '09 – 21 November 2009



Outline

- Critical Information Infrastructure Protection
- Computer Security Incident Response Teams (CSIRTs)
- Warning, Advice and Reporting Points (WARPs)
- How does it all fit together?
- Why is a national “cyber security” effort is required for developing nations?
- Requirements for the developing world
- Community-oriented Computer Security Incident Response Teams (C-CSIRTs)
- Some Links and Resources



Critical Information Infrastructure Protection

- Critical systems rely on a level of interconnection in order to operate
 - Internet
 - Private networks
- Disruptions to the interconnecting networks can severely effect a country's ability to function
 - DDoS attacks
 - Malware
 - Cyber crime
 - Cyber warfare
- National critical information infrastructures must be protected from attack
 - External Threats
 - Internal Threats

Computer Security Incident Response Teams (CSIRTs)

- The first CSIRT structure was created in the US in 1988 in response to the Morris Worm.
- The Primary goals for a CSIRT
 - Monitor for threats
 - Report threats to interested parties (The constituency)
 - Provide support for “incidents”
- The generic structure of a “traditional” CSIRT consists of:
 1. Single Coordinating CSIRT
 2. Many of Regional CSIRTs
 3. Many of Private CSIRTs
- CSIRTs must at least provide incident response services to its constituency.



Warning, Advice and Reporting Points (WARPs)

- Smaller and more focused than CSIRTs
 - A single operator
 - 20-50 members
 - Members are related to each other
 - “Schools in the west of city”
 - “Pharmacists in the east of the city”
- Informal in nature
- Can deliver highly focused cyber security information to its members
- WARPs and CSIRTs compliment each other
 - WARPs never act in isolation
- WARPs are highly cost effective

How does it fit together?

Coordinating CSIRT

Regional CSIRTs

Private CSIRTs

WARPs

Other
Constituents

Military

Large
Corporations

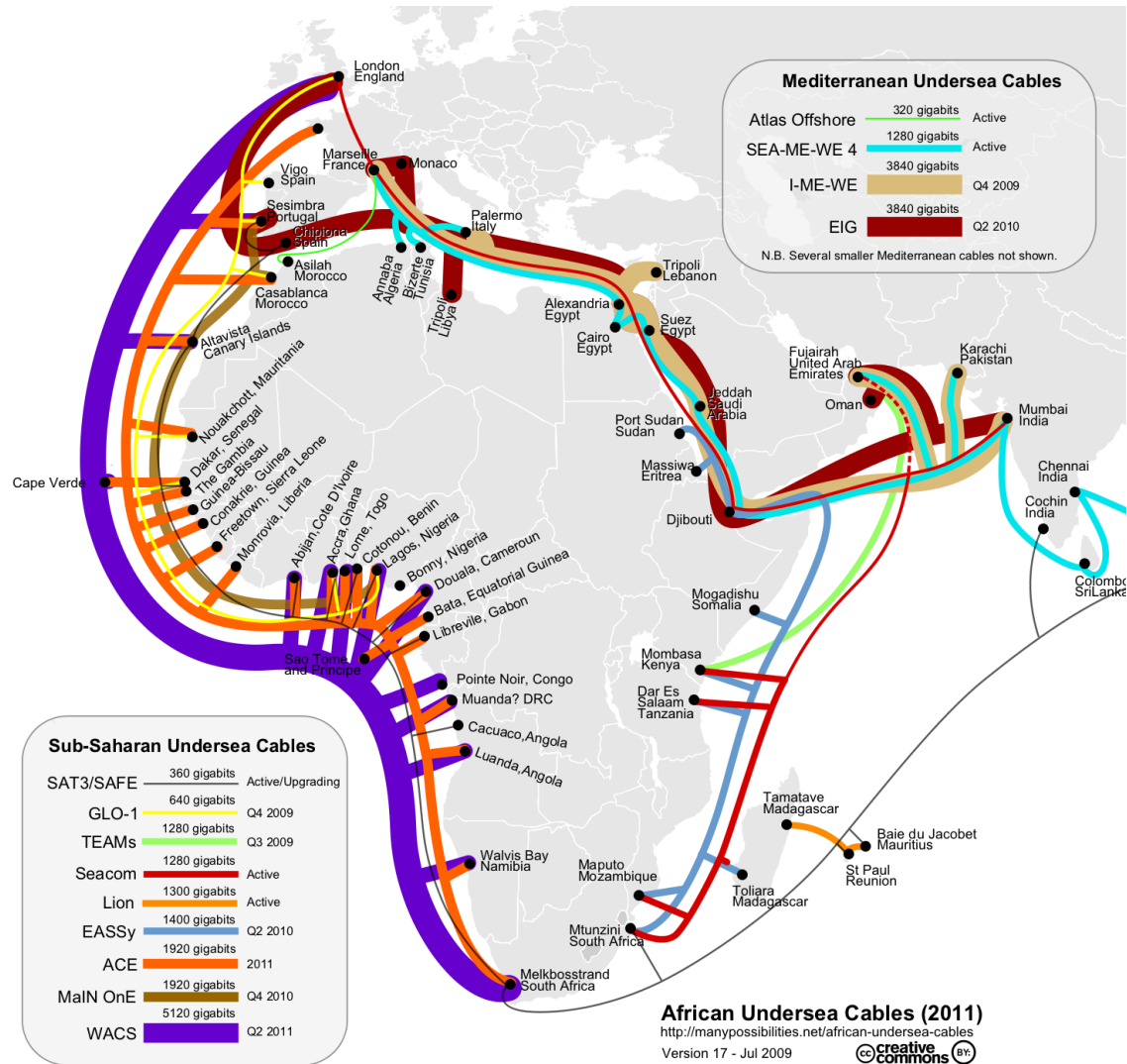
Drawbacks of the “traditional” CSIRT structure

- CSIRTs are very expensive to setup and operate
 - Personnel costs
 - Technology costs
- CSIRT structures are reactive by nature
- Smaller constituents (those without resident IT security professionals) may get “bogged-down” with information.
- Private CSIRTs will generally act in isolation
- WARPS are too small to act in isolation

Why is a national “cyber security” effort is required for developing nations?

- Broadband penetration in developing nations
- Structures are not always in place to prevent abuse of the expanding technology
- Developing nations are seen as a “safe haven” for cyber criminals
- Developing nations may not have the resources to
- A coordinated cyber security effort is essential!

Africa Undersea Cables – 2011



Requirements for the developing world

- Cost effective
- Structures must be dynamically expandable to support increasing connectivity
- Support for Information Exchange and Knowledge Transfer.
- Provide incident response, security advisory and security warning
- Must embrace other technologies to support services
 - e.g. SMS

Community-oriented Computer Security Incident Response Teams (C-CSIRTs)

- C-CSIRTs aim to provide:
 - CSIRT-like protection with WARP-like cost-effectiveness
 - Ability to expand to support new technologies
- Individually functioning security teams which service a “community”
 - 100-200 members
 - “Net of protection”
- C-CSIRTs will attempt to support each other
 - Builds experience
 - Builds knowledge-base
- As the communities grow individual C-CSIRTs can be combined
 - Eventually a national CSIRT structure can develop.
 - Cost, experience, knowledge-base is distributed and developed over time.



Some Links and Resources

- CERT (US)
 - <http://www.cert.org/>
- European Network and Information Security Agency
 - www.enisa.europa.eu/
- Handbook for Computer Security Incident Response Teams (CSIRTs)
 - www.cert.org/archive/pdf/csirt-handbook.pdf
- Warning, advice and reporting point
 - <http://www.warp.gov.uk/>
- Akamai – State of the Internet Reports
 - <http://www.akamai.com/stateoftheinternet/>
- Many Possibilities – African Undersea Cables
 - <http://manypossibilities.net/african-undersea-cables/>

Questions?

