

The Need for Critical Information Infrastructure Protection in the Developing World

Ian Ellefsen and Sebastiaan von Solms
{iellefsen, basievs}@uj.ac.za
Academy for Information Technology
University of Johannesburg, South Africa



Outline

1. Critical Infrastructure vs. Critical Information Infrastructure
2. Cyber Attacks
3. Developing Nations and CIIP
4. Increasing Internet Connectivity
5. Lack of Effective Cyber Security Policies
6. South Africa – Draft Cyber Security Policy
7. Requirements of CIIP in Developing Nations

Critical Infrastructure vs. Critical Information Infrastructure

- Critical Infrastructure
 - “... their incapacitation would have a debilitating impact...”
 - Financial Systems
 - Electricity Distribution
 - Water Distribution
 - Transportation Systems
- Critical Information Infrastructures
 - Many critical systems rely on a level of interconnection
 - Interconnection provided by large networks
 - Private owned networks
 - The Internet
 - DNS
 - TCP/IP
 - Peering
 - Routing
 - Firewalls
 - etc.



Cyber Attacks

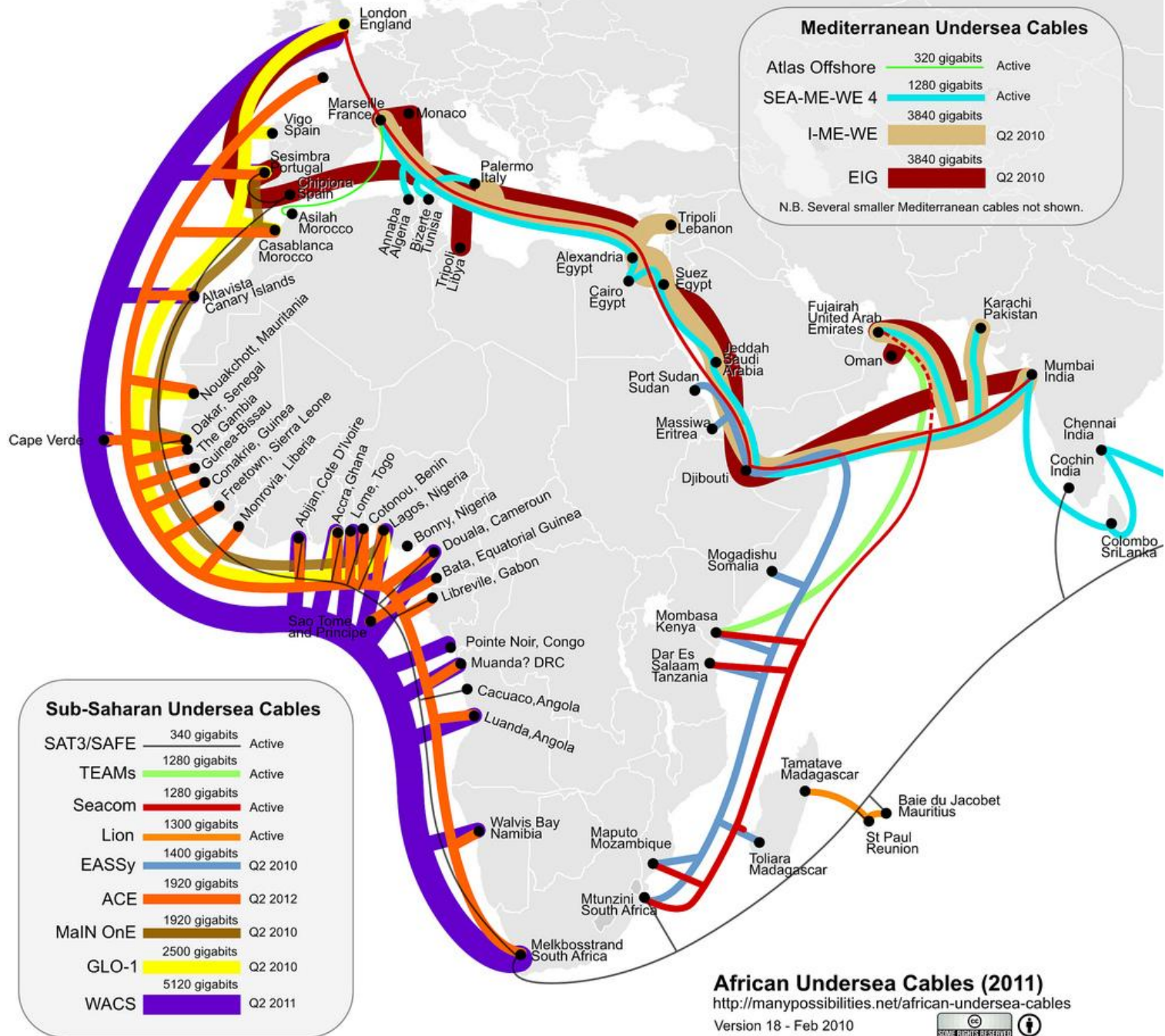
- Information Infrastructures are vulnerable to cyber attacks
 - Distributed Denial of Service Attacks (DDoS)
 - Private Hacktivism
 - Cyber-terrorism
 - State sponsored cyber-warfare
 - Cyber espionage
- Well-known events
 - Georgia (2007)
 - Estonia (2008)
 - DNS Root Servers (2002 & 2007)
 - Google (2009)
- Collateral Damage
 - One event may effect many countries
 - Vulnerability through Interconnection

Developing Nations and CIIP

- Developing nations and Newly Industrialised Nations being used as “staging points” for cyber attacks.
 - Developing nations as defined by the IMF.
- Significant amounts of attack traffic has been observed originating from developing nations.
- Contributing factors:
 - Increasing Internet connectivity
 - Lack of Effective Cyber Security Policies

Increasing Internet Connectivity

- Developing nations are making huge investments into Internet connectivity
- African context
 - Historically very low broadband penetration rates
 - Large amount of investment into high-speed Internet
 - Allows developing nations to remain globally competitive
 - Narrowing Digital Divide
 - Movement towards e-Government services
 - Growth in mobile technologies
- Increases the exposure of Internet users (Private/Commercial/Governmental) to treats
- Incoming and outgoing threats
 - Botnets
 - Malware
 - DDoS
 - Hacking
- Increasing connectivity being utilized for many critical systems.



Attack Traffic by Nation

3rd Quarter 2009

	Country	% Traffic	Q2 09%
1	Russia	13%	1.2%
2	Brazil	8.6%	2.3%
3	United States	6.9%	15%
4	China	6.5%	31%
5	Italy	5.4%	1.2%
6	Taiwan	5.1%	2.3%
7	Germany	4.8%	1.9%
8	Argentina	3.6%	0.8%
9	India	3.4%	0.9%
10	Romania	3.2%	0.6%
–	Other	39%	31%

Source: Akamai Technologies Inc. State of the Internet Q3 2009.
<http://www.akamai.com/stateoftheinternet/>

Lack of Effective Cyber Security Policies

- Never been a need to worry about a coordinated cyber security effort.
 - Threat monitoring
 - Vulnerability Reporting
 - Incident Response
- No real ability to respond to cyber events.
- Cyber criminals can exploit these weaknesses without fear of reprisal.
- South Africa
 - Does not have a coordinated cyber security effort
 - There is some legislation in place which deals with electronic crime
 - DDoS, Hacking, etc.
 - Individuals are responsible for their own cyber security.
 - Draft cyber security policy – February 2010

South Africa – Draft Cyber Security Policies

- Department of Communications
 - 19 February 2010
- Development of Cyber Security Policies
 - United Nations (UN)
 - International Telecommunication Union (ITU)
 - Global Cybersecurity Agenda (GCA)
- Acknowledges lack of effective policies
- Acknowledges existing structures are inadequate
- Makes provision for
 - National Cybersecurity Advisory Council
 - CSIRT structure

Specific Concerns

- Expanding Infrastructure
- Growth in mobile technologies
 - Cellular Networks
 - Wireless Networks
 - Etc.
- Involvement of International Partners, Government, Industry, and Academia
- Bridging the Digital Divide
- Awareness

Requirements for CIIP in Developing Nations

- Cost effectiveness
 - Poorer nations may not have the financial resources to invest into CIIP
- Technical investment
- Information Exchange and Knowledge Transfer
 - Lack of skills
- International Support
 - It is in the interests of international communities
- Awareness
 - Cyber Security Education
- Still and open question

Future Work

- Further investigation into the refinement of the role of CIIP in developing nations.
- Extending and refining the requirements for CIIP in developing nations.
 - Structures
 - Policies
 - Technologies
- Continued research into models which would be appropriate for deployment within developing nations.

Questions?