Submarine Cable Network Security Panel: What We’re Not Discussing Today

Edward Snowden (or WikiLeaks)

Cyber Security Policies or Technology

Can Submarine Cables be Tapped Offshore?
Tools, Methods & Procedures, Options Available to Operators to Enhance Network Security

... Plus, Issues that Remain a Challenge
Submarine Cable Network Security:
Cable Landing Station Security

Threat Protection
- Physical
- Electronic
- Operational

Natural Disasters
- Seismic
- Wind, Flood, Lightning
- Fire

System Failure
- AC/DC Power
- Cooling
- Building Management

Integrated Building Management

- Ballistics rated, forced entry, indirect mortar
- SCIF
- Secure fronthaul
- Min. seismic design criteria category "C"
- 150 mph wind
- Non-combustible construction
- Right-sized and redundant cooling
- Right-sized and redundant cooling
- Integrated Building Management
Submarine Cable Network Security:  
*Product Security – how secure are Submarine Systems?*

- Network/system security delivered in the form of network & access controls.
  - No external access if connected anywhere to Internet or USB key.
- Be careful systems upgrades may be being done with anti-virus s/w.
- Only useful if constantly updated.
- Encryption and communications between OP/ROP, PFE and SLTE.
- ‘Hardened’ software platform based on CIS benchmarks.
- Encrypted communications between OP/ROP, PFE and SLTE.
- ‘Hardened’ software platform based on CIS benchmarks.
- Security of traffic – Confidentiality.
- Security recommendations.
- Password protection & creation.
- Security recommendations.
- Password protection & creation.
- Security recommendations.

- Additional security against other supervisory threats.
  - PFE local control only.
  - BU switching 2nd level authorization.
- Ultimately system security is in the hands of the operators.
- Ultimately system security is in the hands of the operators.
Submarine Cable Network Security: National Interests

- **Balance of national interests**
  - Cable reliability and security (encroachment on cables)
    - Treatment as critical infrastructure
  - Non-interference with other activities (encroachment by cables)
    - Military training, exploitation of natural resources, etc.

- **Increased focus at federal level**
  - Federal Communications Commission coordination
    - Communications Security Reliability and Interoperability Council
      - Reports on routes, landings and intergovernmental coordination
    - FCC Interagency working group
      - Cooperation between agencies that permit cables and other uses of ocean areas
    - [www.fcc.gov/submarine-cables](http://www.fcc.gov/submarine-cables)
  - Increasing spatial awareness
    - [www.marinecadastre.gov](http://www.marinecadastre.gov)
  - Team Telecom
    - Executive branch reviews of security aspects of submarine cables prior to licensing
      - Departments of Homeland Security, Defense, Justice

---

These are my opinions and do not necessarily reflect those of the DoD, US Navy or any other US government office.
• **Initial security reviews**
  – Designed to protect critical infrastructure and communications from damage, disruption and hacking
  – Also designed to prevent unauthorized disclosure of governments’ surveillance activities
  – “Team Telecom” (DHS, DOD, and DOJ) reviews new landing licenses and mergers if landing outside U.S. or if foreign ownership, scrutinizing:
    • Ownership and management access
    • Physical and logical access
    • Equipment and software supply and updates
    • NOC operations – particularly if located outside U.S.
    • Contractor access
  – Similar reviews elsewhere, including India and Australia

• **Security compliance requirements**
  – Team Telecom security mitigation: site visits, annual reports, audits, screening, training
  – Export controls and economic sanctions: dual use equipment, encryption software
  – FCC outage reporting requirements under guise of security

• **Security tensions between governments and industry**
  – Governments want to conduct surveillance without detection
  – Governments are concerned with encryption technology and security appliances that prevent access to communications
  – Creates challenges for industry (e.g., privacy, transparency, customer protections)
Market Size

- Population: 1382 million
- Internet User: 710 million
- Mobile Internet: 656 million
- e-payment %: 64.7%

Internet Content

- ICP License and Certification
- Cloud and CDN Coverage
- Internet Exchange (CHN-IX)
- Submarine Cable / Cross-border

The New Network Security Law

- Passed on Nov 6, 2016
- Effective June 1, 2017

Yali Z. Liu, Vice President, ChinaCache
Submarine Cable Network Security: Consortium Cable Concerns

- Submarine Cables span the globe, no one nation/company can truly ensure high-level security, unless all are committed to doing so.
- While individually companies have taken steps to address such matters, much work remains for consortiums.
- Common Consortium Cable Governance model so far:

  - How could we guarantee security controls including: People, Processes & Technology
  - Is there a need to map Corporate Security Models to Consortium cables?
  - What about Security Operation Centre?

Panagiota Bosdogianni, CTO, OTEGLOBE