SubOptic 2016
www.suboptic.org

Government Surveillance, Hacking, and Network Security:

Dubai
18th-21st April 2016

Emerging Subsea Networks

Celebrating 30 years of SubOptic

What Can Submarine Cable Operators and Their Customers Do?

Kent Bressie

HWG | HARRIS, WILTSHIRE & GRANNIS LLP

Kent specializes in cross-border and national-security regulation of telecommunications networks, investment, and technology and in law-of-the-sea issues. He works extensively in the undersea cable sector and has led various industry-wide regulatory-reform and cable-protection initiatives. He has led many licensing and merger review proceedings for undersea cable operators and carriers before the FCC, Team Telecom, and the Committee on Foreign Investment in the United States. He chairs the undersea cable working group of the FCC's Communications Security, Reliability, and Interoperability Council and has long served as counsel to the North American Submarine Cable Association.

Kent Bressie

Partner and Head of International Practice

kbressie@hwglaw.com

Overview

- Tension between security and surveillance
- Telecom and electronic communications industries: partners and targets
- Increasing demands for surveillance
- Potential abuse by governments
- Consequences for commercial providers
- Limited recourse against governments
- Provider responses: some more effective than others

Network and cybersecurity vs. access

- Fundamental tension exists between:
  - Network security, cyber security, and privacy and
  - Government surveillance activities undertaken in the name of national security and law enforcement.
- For governments to have access, they must deprive bad actors of the ability to conceal their communications.
- Allowing for such access and the gathering of data can, themselves, create network and cyber security risks and new targets.

An attractive target

- Fiber-optic technology and encryption techniques have made surveillance and hacking of communications traffic on contemporary submarine cables more difficult, but not impossible, as compared with analogue, coaxial cables with unencrypted communications—as evidenced by disclosures in the mid-2000s about U.S. intelligence agencies using beam splitters to access communications from trans-Pacific submarine cables.
- The United States pioneered tapping of submarine cables with Operation Ivy Bells, which targeted Soviet cables in the Sea of Okhotsk in the 1970s, and is alleged to have equipped its more contemporary submarine, the USS Jimmy Carter, with fiber-tapping capabilities.
- More recently, reports surfaced in 2015 claiming that Russian ships were tracking and potentially tapping submarine cables serving the United States.

An attractive target

- Certainly, submarine cables remain a focal point for network security and surveillance, not least of all because they aggregate so much information in discrete locations.
- They remain vitally important to national security and economic activity, and they carry the vast majority of the world's international Internet, voice, and data traffic—a fact that makes them potentially attractive targets for causing harm and for gathering information to prevent harm.
- Developments in "fiber tapping" have made access to a fiber-optic cable's communications stream feasible.
- Applications of vast computing power and storage capabilities for breaking encryption and searching data have also opened up the possibility of access to vast communications streams that can provide law enforcement and intelligence agencies with reams of data.

Aftermath of September 11th

- Tension between security and access has become more acute in the last 15 years due to:
  - September 11 attacks in the United States and subsequent terrorist attacks around the world;
  - Wars (and their aftermaths) in Afghanistan, Iraq, Libya, and Syria and in regions occupied or threatened by the Islamic State; and
  - A rising tide of cyberattacks around the world.
- Post-September 11, many governments have significantly expanded their surveillance activities to detect and monitor threats.

Demands for access have only grown more acute

- The high profile terrorist and cyber-attacks of the last 15 years ensure that security remains an overwhelming policy priority for many countries, with calls for more intensive surveillance after each new incident.
  - Following the attack on *Charlie Hebdo* offices in Paris, France proposed to adopt a French version of the USA PATRIOT Act.
  - A number of intelligence agencies and observers have renewed calls for a back door similar to the Clipper Chip, a chip set developed by the U.S. National Security Agency ("NSA") that used an encryption key escrow that provided governments with a back door to access encrypted communications.
  - The UAE Government proposed a ban on BlackBerry Messenger following the assassination of a Hamas official in Dubai in 2010 pending negotiation to obtain access to encrypted messages.

Demands for access have only grown more acute

- In 2016, Microsoft continues to challenge U.S. Federal Bureau of Investigation (“FBI”) attempts to access data stored in its Irish data center and assertions that the FBI can compel disclosure of data stored anywhere in the world if the provider is based in the United States.
- Also in 2016, the FBI remains embroiled in litigation with Apple, seeking to force Apple to unlock iPhones, particularly one used by one of the perpetrators of a bombing in San Bernardino, California in 2015.

Access and data can easily be abused

- There is disagreement about what does and should constitute a bad actor sufficient to justify surveillance. Is a bad actor:
  - An imminent security threat, such as a terrorist bomber or a proliferator of nuclear or biological weapons?
  - An economic competitor?
  - A government critic, political dissident, democracy activist, or a non-governmental organization like Greenpeace or Amnesty International?
- Once access is created and data is gathered, there is always a temptation to use it—or misuse it for other purposes.
- Government overreaching can undermine customer confidence, as it has done with U.S. cloud services providers following disclosures by WikiLeaks and Edward Snowden.

Telecoms and electronic communications industries: uneasy partners, targets, or both?

- Telecommunications and electronic communications providers have long been caught in the middle of government surveillance activities.
- Governments have sometimes enlisted the telecom and electronic communications industries—willingly or not—to ensure access and to protect the confidentiality of such surveillance.
  - AT&T and Verizon were accused of breaking U.S. law to cooperate with U.S. Government surveillance activities and received retroactive immunity in 2008.
- In other cases, the telecommunications and electronic communications industries have been the target of surveillance.
- Government security efforts will likely continue to focus on telecom and other electronic communications networks given the integration of electronic communications in almost all aspects of contemporary life.

Edward Snowden and WikiLeaks disclosures

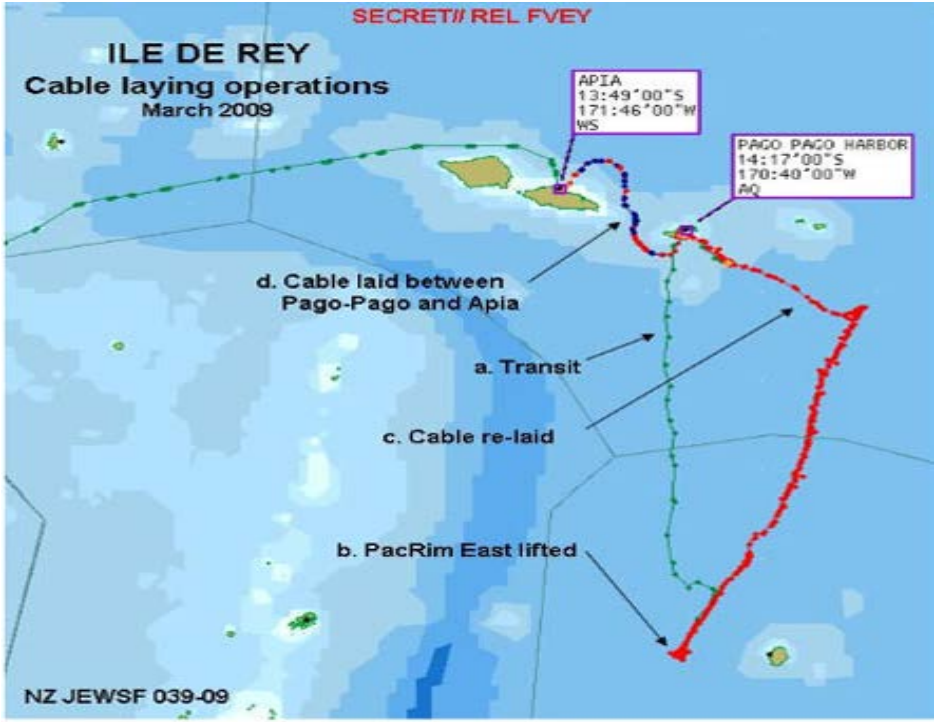
- Edward Snowden and WikiLeaks are largely—but not entirely—responsible for new public awareness of surveillance and spying.
  - Snowden's 2013 disclosures focused on U.S. surveillance and spying methods.
  - WikiLeaks' disclosure of U.S. diplomatic cables in 2010 included significant classified information gathered through surveillance.
  - Disclosures about hacking of submarine cable traffic first surfaced in 2007 in connection with the Room 641A program.
  - U.S. programs have received the most publicity and are the most extensive, but they are not unique.
  - Spying is also not limited to the "Five Eyes."

Key programs

- **ECHELON**: signals intelligence collection and analysis network of the “Five Eyes” (Australia, Canada, New Zealand, the United Kingdom, and the United States) started in the 1960s to focus on diplomatic and military traffic.
  - Later expanded to include private and commercial traffic.
  - Focuses on exploiting satellite communications.
- **Xkeyscore**: NSA data-retrieval system allowing access to telephone calls, emails, social media and meta data. Has been shared with Five Eyes, Germany (its biggest paying customer), and Sweden.
- **PRISM**: NSA program collecting stored Internet communications of non-U.S. persons held by major U.S. Internet companies.
- **Room 641A**: interception facility on AT&T premises in San Francisco, using beam splitters in fiber-optic networks to access IP-based traffic.

2015 disclosures re New Zealand

- In March 2015, the *New Zealand Herald* broke the story of New Zealand's Government Communications Security Bureau ("GCSB") spying on Fiji, French Polynesia, Kiribati, Nauru, New Caledonia, Samoa, the Solomons, Tonga, Tuvalu, and Vanuatu in exchange for access to Xkeyscore.
- The *Herald* released documents showing the tracking of the installation of Blue Sky's ASH and SAS cables, which GCSB feared would deprive it of access by replacing satellite connectivity.



Surveillance and the U.S.-China relationship

- Much of U.S. surveillance in the Pacific region is driven by concerns about China.
  - United States has long sought to preserve U.S. naval power in the Pacific.
  - United States has watched warily as China has given significant development aid and initiated many commercial projects in the Pacific islands.
- These concerns are part of a larger shift of importance to the Asia-Pacific region and China's growing influence in regional and global organizations, *e.g.*, Asian Infrastructure Development Bank.

Consequences for telecom and electronic communications providers

- Revelations about spying have placed electronic communications providers (including telecom carriers) in the middle.
  - Carrier compliance with government requests has resulted in an erosion of customer confidence, particular for U.S.-based networks and cloud computing providers.
  - Customers and NGOs have filed lawsuits against carriers.
- Providers must comply with domestic laws that enable surveillance.
  - Failure to comply can lead to:
    - Prosecution and fines
    - Loss of operating licenses
    - Loss of government contracts

Limited recourse for government overreaching

- Telecommunications providers have limited recourse for government overreaching.
  - They can mount legal challenges a government's request for cooperation.
    - Not permitted in many jurisdictions.
    - Can be extremely difficult, such as when involving the procedures of the U.S. Foreign Intelligence Surveillance Court.
  - They can seek legislation granting immunity from private lawsuits.
- Consumers and residents of foreign countries have little or no recourse; foreign governments can only raise objections at the diplomatic level or expel suspected spies.
- Typically, foreign governments can only raise objections at the diplomatic level or expel suspected spies, although the new EU-US Privacy Shield bars the United States from conducting "indiscriminate" national security surveillance of Europeans and a U.S. Department of State ombudsman to police compliance.

Provider responses to surveillance and spying

- Governments will continue to conduct surveillance and hack and spy as they always have.
- Although providers have limited leverage in challenging domestic legal requirements, they can bolster defenses against hacking.
  - Some measures are more effective than others.
  - Other measures are “for show” politically and do little to limit surveillance efforts of other governments.

Bypass infrastructure

- In response to revelations that the U.S. intercepted telephone conversations of Brazilian President Dilma Rousseff, Brazil:
  - Advocated for bypass measures to avoid routing communications through the United States, and
  - Promoted new submarine cables that would link Brazil directly to Europe
- Bypass strategies ignore the fact that most government spy agencies operate beyond the boundaries of their home countries.
- Bypass is not a viable option if customers want to access content stored in a country accused of spying.
- Given the proliferation of new cables on the U.S.-Brazil route—including BRUSA, Monet, and Seabras-1—one must wonder whether the Brazilian Government's official policy is getting any traction.

Data localization and data sovereignty

- Data localization requires that data of a country's residents or citizens be stored in that country.
  - Brazil also proposed this as a remedy for U.S. spying.
  - It is technically inefficient and potentially more expensive.
  - It is disliked by civil libertarians and democracy activists, as it enables political oppression of dissidents.
  - The United States has strongly opposed the adoption of data localization requirements and has sought to include provisions in the Trade in Services Agreement to mandate the free flow of data.

Encryption

- Government surveillance agencies remain highly concerned about the proliferation of encryption technology, worrying that bad actors will "go dark," *i.e.*, communicate only with encrypted communications so as to avoid detection altogether.
- U.S. Government had long tried to assert that privately-developed encryption technology was classified and/or stolen, and it still subjects U.S.-origin encryption source code to U.S. export controls.
- Companies such as Apple and Yahoo have promoted encryption, including end-to-end encryption in which a company could not provide the government with a master key.

Robust network security and cybersecurity

- Many operators make themselves targets for hacking by bad actors and intelligence agencies by failing to maintain robust network security and cybersecurity policies and procedures.
- Operators can make themselves less attractive targets and better protect their businesses by adopting and implementing:
  - Security and privacy programs;
  - Vendor assurance programs for hardware and software;
  - Incident response plans;
  - Policies defining how threat and incident information will be shared with governments; and
  - Customer assurance programs.

Transparency

- U.S. technology companies such as Microsoft, Yahoo, Google, and Cisco—all competing to maintain customer confidence—have systematically sought court rulings and negotiated with the U.S. Government to disclose statistics regarding U.S. law enforcement requests.

International convention?

- Microsoft has called for the adoption of an international convention on government access to data, which would
  - Narrow access to address clear-cut law enforcement and national security concerns, and
  - Speed cross-border sharing of information that might otherwise be rendered less valuable as a result of procedural delays.

For further information, please contact:

Kent Bressie
Harris, Wiltshire & Grannis LLP
1919 M Street, N.W., Suite 800
Washington, D.C. 20036-3537
U.S.A.
+1 202 730 1337
kbressie@hwglaw.com
www.hwglaw.com

SubOptic 2016
www.suboptic.org

Dubai
18th-21st April 2016

Emerging Subsea Networks

Hosted by e-marine

Celebrating 30 years of SubOptic