COPING EFFECTIVELY WITH NATIONAL-SECURITY REGULATION OF UNDERSEA CABLES

Kent Bressie (Wiltshire & Grannis LLP)
kbressie@wiltshiregrannis.com

Abstract: Responding to the threats of terrorist and cyber attacks and other armed conflicts, governments have significantly increased their scrutiny of undersea cable infrastructure and services to protect national security, ensure access for surveillance purposes, and secure government communications. While intended to prevent disruption of communications, these measures can be very disruptive to infrastructure owners and service providers by imposing costly compliance burdens, delaying market entry and investment, and interfering with procurement and contracting decisions, as evidenced by recent actions of the Australian, Indian, and U.S. Governments. Such efforts can also serve as cover for trade protectionism and erode market-opening efforts undertaken following the landmark 1997 World Trade Organization agreement in basic telecommunications services. National security regulation and trade controls now involve far more than an ownership review during the initial licensing phase. Governments increasingly regulate equipment and software supply, maintenance arrangements, and physical and logical access to cable-system facilities—particularly cable stations—and impose foreign-policy-based trade controls on services and equipment transactions.

Following the September 11, 2001, terrorist attacks, subsequent attacks in other countries, and high-profile cyberattacks, governments have worried increasingly about vulnerabilities of undersea cable infrastructure and communications to terrorist attacks. Suddenly, cable cuts in the Mediterranean, the Gulf, and Southeast Asia were assumed to be potential terrorist incidents rather than the results of conflicts with other seabed users.

Governments have responded by focusing increasingly on infrastructure security and information security for undersea cable networks and surveillance capabilities for communications transported by such networks. Governments have adopted new regulatory reviews and requirements for undersea cable systems landing in their territories. They also continue to scrutinize mergers and acquisitions affecting undersea cables, exports of undersea cable equipment and technology, and commercial transactions involving targeted countries, entities, and persons.

The resulting increase in national-security regulation and foreign policy-based trade controls has the potential to increase costs, create regulatory delays, and limit revenue opportunities. Industry members need to address such concerns at the earliest stages in system financing, business planning, procurement, and establishment of operational processes. As ever, industry needs to consult with governments proactively to prevent misguided and unnecessarily burdensome regulation.

1. DEFINING "NATIONAL SECURITY"

Nations do not agree on the definition of "national security," and none exists under international law. While some treaties refer to "security," they generally do not define it. For example, the United Nations Convention on the Law of the Sea distinguishes "security" from "defense" but defines neither.[1] Similarly, the World Trade Organization ("WTO") agreements contain security exceptions but they do not

define "security." The WTO General Agreement on Trade in Services contains exceptions for: (1) protecting "public order," where "a genuine and sufficiently serious threat is posed to one of the fundamental interests of society" and (2) protecting "essential security interests."[2] The discretion to define "national security" is seen as a key indicator of sovereignty—one that most countries are loathe to have circumscribed. Some countries view it in terms of military or political security. Others also define it in economic and/or cultural terms.

Nevertheless, with respect to undersea cables, there is some commonality across governments in terms of the risks that they seek to mitigate. Undersea cables fall within most definitions of "critical infrastructure"—infrastructure and assets vital to national security, governance, public health and safety, economy, and public confidence.[3]

2. THREATS TO TELECOMMUNICATIONS INFRASTRUCTURE AND TRANSMISSIONS

While there is no established definition of national security, and most governments are keen not to have one imposed on them, governments do often identify the same kinds of threats to national security. These threats include:

- Malicious and terrorist acts, such as: attacks on physical network facilities; cyberattacks (*e.g.*, malware, phishing, denial-of-service attacks, viruses, and botnets); unauthorized access (*e.g.*, back doors, Trojan viruses); and government and industrial espionage;
- A lack of effective access to communications stream for surveillance purposes;
- Excessive reliance on infrastructure supplied or owned by foreign companies, which some governments see as undermining self-sufficiency; and
- Activities deemed objectionable for foreign-policy reasons, including economic or military support for a targeted country, and supply of infrastructure or technology that could enhance political control over citizens by a targeted country.

Governments also worry about non-malicious sources of cable damage that could interrupt government or commercial communications viewed to have national importance, including:

- Vessel anchors;
- Commercial fishing activities, particularly driftnets and gillnets;
- Earthquakes; and
- Tsunamis.

3. NATIONAL SECURITY VS. ECONOMIC PROTECTIONISM

Sometimes, it is difficult to distinguish security measures from protectionism designed to shelter domestic companies from foreign competition. For example, the United States adopted its principal law governing undersea cables—the Cable Landing License Act of 1921—in response to a concern that a British-led consortium would dominate the U.S.-Brazil route for telegraph cables and disadvantage an American competitor. President Wilson's administration, however, justified the legislation as necessary to "protect the national territory" and suggested that it was necessary to counter Communist influences during the Red Scares.

For governments that define "national security" in terms of economic security, however, protectionism directly serves

"national security." The Indian Government's recent indigenous innovation initiatives in the area of telecommunications network equipment—including undersea cable systems—is premised expressly on the concept that development of domestic equipment production strengthens national security.

4. UNDERSEA CABLE ACTIVITIES SCRUTINIZED BY GOVERNMENTS

Government scrutiny and regulation of undersea cables for national-security and foreign-policy reasons affects virtually every aspect of an undersea cable's ownership, financing, operation, and maintenance:

- System ownership
- System financing: choice of lenders and intermediary financial institutions
- System management, employees, and contractors with access to infrastructure, particularly at cable stations and network operations centers ("NOCs")
- Network design
- Landing party arrangements
- NOC operations and back-up NOC arrangements
- Equipment and software supply
- Equipment upgrades, software updates and patches, spare plant, and repairs
- Outsourcing and offshoring arrangements for operator activities and data
- Maintenance and restoration arrangements
- Storage of spare plant
- Communications stream (for surveillance purposes) and data about surveillance requests
- Exports of equipment, technology, and software (for foreign-policy-based export controls and boycotts)
- Financial transactions for goods or services (for foreign-policy-based economic sanctions and boycotts)
- Data retention capabilities (which sometimes conflict with privacy regulation)
- Infrastructure and information security plans
- Surveillance and wiretapping capabilities

5. RISK-MITIGATION METHODS AND REMEDIES USED BY GOVERNMENTS

a. Initial Security Reviews and Mitigation Agreements

Historically, the security component of initial licensing reviews focused mostly on foreign ownership. Where regulations have not been adopted, commitments are memorialized in the form of security agreements and assurances letters and enforced through audits. The so-called "Team Telecom" in the United States—the Departments of Defense, Homeland Security, and Justice—pioneered this approach, but it is not catching on elsewhere.

For example, the Indian Government initially mandated vendor-operator agreements but now only encourages use of template agreements. The Australian Government has pursued development of a notification process and risk assessments for infrastructure purchases and network upgrades and modifications that may have national security implications.

b. Subsequent Security Reviews of Ownership Changes

In many countries, the acquisition of an existing business by a foreign investor triggers a separate foreign-ownership and national-security review.

- ***China***: Pursuant to a 2011 State Council circular, the National Development and Reform Commission and the Ministry of Commerce lead security reviews of inward foreign investment in enumerated sectors, including critical infrastructure.[4]

- ***Russia***: The Federal Antimonopoly Service reviews foreign investment affecting national defense and state security.[5]

- ***United States***: The Committee on Foreign Investment in the United States reviews foreign acquisitions of existing U.S. businesses.[6]

- ***India***: The Foreign Investment Promotion Board reviews national security implications of foreign investment.[7]

- ***France***: The Ministry of Economy, Finance, and Employment reviews mergers and acquisitions in 11 sectors implicating national security, including a number touching on telecommunications services and equipment.[8]

- ***Britain***: The Secretary of State for Business, Innovation & Skills may intervene in merger cases on national security grounds.[9]

Of course, many countries (*e.g.*, Mexico) still maintain statutory or constitutional limits on foreign investment, regardless of national security concerns.[10]

c. Procurement Restrictions

After years of privatizations and new private investment, governments are getting back into the business of telecommunications. Their ownership and operation of next-generation networks—such as Australia's National Broadband Network, owned through NBN Co., and the First Responder Network Authority in the United States—gives them direct authority over procurement and security issues. For example, such control permitted the Australian Government to initially block Huawei participation in the NBN.[11] Unless specifically scheduled, these entities are not subject to the WTO Agreement on Government Procurement, which otherwise ensures access by foreign suppliers to government procurements.

Governments also use their informal persuasive powers to influence procurement decisions by private network owners. In 2010, the U.S. Government was seen to exert pressure on Sprint not to source mobile network upgrade equipment from Chinese supplier Huawei due to U.S. Government security concerns, and Sprint ultimately sourced that equipment from Alcatel, Ericsson, and Samsung.[12]

d. Surveillance

Governments continue to impose new surveillance requirements, both to protect national security and to serve the needs of domestic law enforcement. Some of these initiatives have foundered, as in Canada, where privacy advocates and provincial government officials objected strongly to federal legislation proposed in Bill C-30.[13] Other initiatives have been approved by national courts, as in the U.S. Supreme Court's recent decision upholding surveillance—pursuant to the FISA Amendments Act—of non-U.S. persons reasonably believed to be outside the United States.[14] In general, these

requirements are not specific to undersea cables, though governments remain very keen on using cable stations as access points for surveillance.

e. Disclosure or Escrow of Source Code and Product Designs

Governments have sometimes sought disclosure or escrow of source code and product-design documents, on the theory that they could be examined to help investigate or remediate a security breach. For example, the Indian Government had sought to impose a template vendor security agreement for purchases of foreign telecommunications equipment and software, mandating escrow of source code and product designs to be accessed in certain security-related circumstances. In other cases, suppliers have offered to share source code as a way of gaining market access and assuring the relevant government re product security. Source code continues to generate controversy, as it touches on the long-running debates about the security of open-source code and what constitutes open-source, and reveals inconsistencies in positions by both governments and equipment/software suppliers.

f. Local Content Requirements

Some governments assert that local sourcing of equipment strengthens national security and therefore impose local content requirements for equipment procurements. In some cases, the restrictions apply only to government procurements. In other cases, the restrictions apply to private enterprises. For example, through a series of draft national policies on telecommunications, electronics, information technology, and national security, the Government of India has advocated for local-content requirements and indigenous innovation to bolster the Indian economy and reduce security risks.

g. Data Reporting and Inventories

To identify patterns of activity and possible terrorist incidents, governments increasingly require reporting regarding outages, restoration arrangements, and other useful data. Governments have also conducted inventories of deployed network equipment and software. Australia commenced such a review in 2008, and the United States commenced such a review in 2011 (led by the Departments of Commerce and Defense).

6. EXPORT CONTROLS, ECONOMIC SANCTIONS, AND BOYCOTTS

Governments also pursue their foreign-policy and security objectives by restricting exports of goods, technology, and software to particular countries and end users (export controls) and by broadly restricting financial, export, and services transactions with particular countries, organizations, and individuals (economic sanctions).

Export controls generally come in two flavors: (1) restrictions on dual-use goods, technology, and software (commercial items that could have military applications) and (2) restrictions on military items. Undersea-cable equipment and software is generally “dual use” and subject to minimal controls, except where economic sanctions apply. Many developed countries belong to the Wassenaar arrangement, whose members agree to maintain national-level export controls, adopt best practices, and report on transfers to countries outside the arrangement.

Governments impose restrictions on financial and economic transactions

(regardless of any export of a good or technology) and facilitation via third parties of transactions that cannot be undertaken directly. Some sanctions are multilateral, undertaken in response to U.N. resolutions (*e.g.*, apartheid-era South Africa, Iran, and North Korea), while others are regional (*e.g.*, Arab League boycott of Israel) or unilateral (*e.g.*, U.S. sanctions against Cuba and U.S. and EU sanctions against Myanmar (partly lifted), Libya (mostly lifted), and Syria). U.S. and E.U. sanctions are often extraterritorial—applying to nationals wherever located—and are sometimes telecom sector-specific. The United States in particular views third-country activity in sanctioned countries as a security risk.

7. CONSEQUENCES AND RESPONSES

Government scrutiny and regulation of undersea cable activities has significant consequences for undersea cable operators, equipment suppliers, and their investors and customers. This regulation increases operating costs by imposing higher compliance costs (which could grow depending on choice of investor/lender, supplier, contractor, or customer), reducing competition in supply of equipment or services (where particular suppliers and contractors are barred), and causing losses of revenue. It also imposes project delays and increases regulatory uncertainty.

All undersea cable-related businesses should familiarize themselves and their personnel with national security regulation and foreign policy-based controls for the relevant jurisdictions. They should also recognize that the system owner has ultimate responsibility for national security matters. In general, the system owner cannot outsource these obligations to the supplier or contractor, though the supplier or contractor can (and in many cases, really must) assist the system owner in addressing national security concerns. Undersea cable-related businesses should not wait until after signature of a construction and maintenance agreement, supply contract, or maintenance agreement, or until commencement of system pre-sales, before grappling with these issues. They should proactively review their prospective export and financial transactions for compliance with the relevant national export controls and economic sanctions. And they should consult with expert in-house personnel or outside counsel/consultants with direct experience. Most regulation in this area involves unwritten rules and practices.

System owners should also consider undertaking additional best practices. They should conduct risk assessments of suppliers of equipment, software, maintenance, data outsourcing, and other support services during the procurement phase, and of investors and lenders during the funding phase.

Suppliers of equipment, technology, and services should also consider undertaking additional best practices. They should address security considerations in supply-chain management and customer assurance programs. They should also engage with specific customers about national security issues.

To limit the impact of these regulatory burdens on undersea cables, the undersea cable industry needs to engage more proactively with governments regarding proposed security-related regulatory programs before they are implemented. Governments in particular need to understand that information about undersea cable systems must be made public in order to minimize damage to cables through non-malicious acts. Industry also needs to continue to urge governments to

take a more holistic approach to cable protection (looking at both malicious and non-malicious risks) likely to be more effective and to encourage workable solutions (*e.g.*, mesh networks and diversity).

REFERENCES

[1] United Nations Law of the Sea Convention, art. 19.2(c), Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force on Nov. 16, 1994) ("UNCLOS").

[2] General Agreement on Trade in Services, arts. XIV(a), XIV *bis*, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, The Legal Texts: The results of the Uruguay Round of Multilateral Trade Negotiations 284 (1999), 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994).

[3] *See, e.g.*, 50 U.S.C. App. § 2170(a)(6) (defining critical infrastructure, for purposes of reviewing the acquisition of an existing U.S. business engaged in interstate commerce by the Committee on Foreign Investment in the United States, as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security").

[4] Office of the State Council's Notice on the Establishment of a Security Review System for Foreign Investment in, and Acquisitions of, Domestic Enterprises, Office of the National Council Circular (2011), No. 6.

[5] Federal Law on Foreign Investment in the Russian Federation, No. 160 (1999), 39 I.L.M. 894 (2000).

[6] Section 721 of the Defense Production Act of 1950, *codified as amended* 50 U.S.C. App. § 2170.

[7] Foreign Exchange Management Act, Act No. 42 of 1999; Foreign Exchange Management (Transfer or Issue of Security by a Person Resident Outside India) (Sixth Amendment) Regulations, 2012.

[8] French Monetary and Finance Code, art. L151-3.

[9] Enterprise Act, 2002, §§ 42-58.

[10] *See, e.g.*, Mexican Foreign Investment Law, art. 6 (1993).

[11] Geoffrey Barker and David Ramli, "China's Huawei Banned from NBN," *Australian Financial Review* (Mar. 24, 2012).

[12] Joann S. Lublin and Shayndi Rice, "Security Fears Kill Chinese Bid in U.S.," *The Wall Street Journal* (Nov. 5, 2010).

[13] John Ibbitson, "Harper Government Kills Controversial Internet Surveillance Bill," *Globe and Mail* (Toronto) (Feb. 11, 2013).

[14] *Clapper v. Amnesty International USA, Inc.*, 568 U.S. ____ (2013).

