OFFSHORE ENERGY EDITION

submarine telecoms

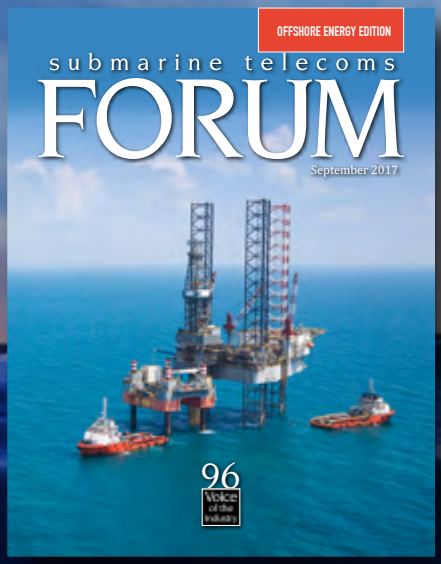
FORUM

September 2017

96

Voice of the Industry

IN THIS ISSUE...



NEW MEASURES AND GUIDELINES IMPLEMENTING CHINA'S CYBERSECURITY LAW COULD BURDEN SUBMARINE TELECOMMUNICATIONS NETWORKS

RESTRICTIONS COVER CROSS-BORDER TRANSFERS OF OPERATIONAL AND SECURITY DATA, MARINE ENVIRONMENTAL DATA, AND GEOGRAPHIC INFORMATION

BY KENT BRESSIE

To implement the People's Republic of China's new cybersecurity law, which took effect on June 1, 2017, the Cybersecurity Administration of China adopted new implementing measures on June 1, 2017, and proposed further guidelines on May 27, 2017, that could restrict the cross- border transfer of key data created or stored by submarine cable operators, suppliers, and survey companies to design, install, operate, and repair submarine cables, including construction, operational, and security data, marine environmental data, and geographic information for telecommunications networks. Cross-border exchanges of data are a fundamental part of the submarine cable industry, as the vast majority of submarine cables themselves land in or transit multiple jurisdictions and have owners located in multiple jurisdictions. Submarine cable operators routinely transfer seafloor surveys to owners and contractors during route development and system status, alarm, and fault data to owners, contractors, customers, and network operations centers during the operational phase. If implemented in a stringent manner, these new requirements could render submarine cable installation, operation, and repair significantly more costly and increase repair times. Given the expansive views of the PRC government regarding its maritime jurisdiction within its exclusive economic zone and ocean areas subject to jurisdictional disputes, the new measures and guidelines could complicate the installation and maintenance of submarine cables landing in or transiting near the PRC.

THE CYBERSECURITY LAW

The PRC adopted the Cybersecurity Law on November 7, 2016, in order to enhance network security and the security and privacy of PRC citizens. The Cybersecurity Law imposes data security requirements on network operators and critical information infrastructure ("CII") operators. Many of the requirements will sound familiar to operators who have been subject to a review or mitigation by the U.S. "Team Telecom" agencies, although the PRC requirements are much broader and would capture most companies with IT systems, not just telecommunications network businesses, in the PRC.

- The Cybersecurity Law defines "network operators" to include "systems comprised of computers and other information terminals and related equipment" that gather, store, transmit, exchange, and process information.
  - This broad definition captures not only owners of electronic communications networks but also any owner or operator of IT systems gathering, storing, or transmitting data in the PRC.
- Network operators must adopt and maintain network security measures, develop incident response plans for data breaches, and provide technical assistance to public security agencies in national security and criminal matters.

If implemented in a stringent manner, these new requirements could render submarine cable installation, operation, and repair significantly more costly and increase repair times.

- It defines "CII operators" to include businesses providing public communications and information services, energy, transportation, water resources, finance, public services, and electronic communications as well as businesses owning or operating infrastructure that, if destroyed or impaired, would pose a serious threat to national security or the social or economic well-being of the PRC.
  - CII operators must adopt and implement personnel screening and training, submit to national security reviews when purchasing network products and services that could affect national security, and conduct annual inspections.
  - Article 37 requires CII operators to comply with data localization requirements, storing in the PRC any personal information and other "important data" collected or generated in the PRC.

NATIONAL SECURITY REVIEWS FOR CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION AND "IMPORTANT DATA"

To implement the Cybersecurity Law's restrictions on cross-border data transfers, the Cybersecurity Administration adopted its Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data (the "Measures") on June 1, 2017, although they will not take effect until December 31, 2018.

- **Expanded Scope**. To transfer personal information or "important data" outside the PRC, and only for "legitimate business reasons," the Measures extended the data localization requirements in Article 37 of the Cybersecurity Law to include network operators as well as CII operators, requiring them to submit a proposed cross-border data transfer for national security review by the "competent regulatory authority."
- **Certain Transfers Prohibited**. If the cross-border transfer would trigger a concern specified in Article 9 of the Cybersecurity Law, the transfer would be prohibited. Article 9 concerns include: a risk to the PRC political system or economic, scientific or technical, national defense, societal, or public interest; the absence of consent of the data subject; and other circumstances specified by the PRC government. Failure to comply with these requirements could subject an enter-

prise to a loss of income, fines (on the enterprise and its management individually), and a suspension of operations.

"IMPORTANT DATA" INCLUDE PLANNING, CONSTRUCTION, OPERATIONAL, AND SECURITY DATA INVOLVING TELECOMMUNICATIONS INFRASTRUCTURE

Article 7 of the Measures requires a security assessment by the "competent regulatory authority" prior to the cross-border transfer of data on "cybersecurity- related information like security vulnerabilities or specific security measures of critical information infrastructure." The Information Security Technology – Guidelines for Data Cross- Border Transfer Security Assessment (the "Draft Guidelines"), released on May 27, 2017, propose to designate the Ministry of Industry and Information Technology as the "competent regulatory authority" for a broad range of communications data, including:

- Planning and Construction Data. These data include information about planning, design, and construction of telecommunications networks, disaster management, equipment geographical location, network topology, route information, equipment procurement.
- Operational Data. These data would include equipment and software configuration information, traffic flow data, network status information, maintenance logs, and system user information.
- Security Data. These data would include network and information security management data, alarm data, access logs, security audit records, security contingency plans, unauthorized use data, billing records, and personal communications data.

"IMPORTANT DATA" INCLUDE MARINE ENVIRONMENTAL DATA AND GEOGRAPHIC INFORMATION

Article 7 of the Measures requires a security assessment by the "competent regulatory authority" prior to the cross-border transfer of data on "the marine environment or sensitive geographic information, or cybersecurity-related information like security vulnerabilities or specific security measures of critical information infrastructure."

- **Marine Environmental Data**. The proposed Draft Guidelines propose to designate the State Oceanic Administration as the "competent regulatory authority" for marine environmental data, including:
  - "Observations and statistical data on submarine topography, marine hydrology, marine meteorology, underwater acoustic environment and marine physical field;
  - The temperature of the sea, water, sediment, tide, current measured data and related results; and
  - Unpublished marine ecological environmental monitoring data."
- **Geographic Information**. The Draft Guidelines propose to designate both the National Administration of Surveying, Mapping, and Geoinformation and State Oceanic Administration as the "competent regulatory authorities" for geographic information, including information about the location of communications facilities and attributes of communications lines.

LIMITED WINDOW FOR REVISION

The Measures and the Draft Guidelines would impose significant burdens on submarine cable operators, and they leave many questions unanswered. As the Measures do not take effect until December 2018, and because the Draft Guidelines have not yet been finalized, industry nevertheless has an opportunity to seek clarifications and refinements to limit the burden of the Cybersecurity Law.

Kent Bressie *is a partner with Harris, Wiltshire & Grannis LLP and heads its international practice. An expert on telecommunications, international trade and investment, and national security regulation, he represents communications and technology companies and investors in a wide variety of cross-border and domestic regulatory and commercial matters. He works extensively in the undersea cable sector and represents operators, suppliers, investors, and the North American Submarine Cable Association. His work includes: national security and foreign investment; telecoms licensing; corporate and commercial agreements for construction and maintenance, capacity sales, system supply, landings, and financing; environmental permitting; market access; and cable protection and the law of the sea.*