In the Shadows of Global Fiber Networks:

Data Heist, Spying and Sabotage

Terrestrial optical fiber cables together with the undersea cable infrastructure are the critical components of global communication networks. They offer high-speed data transmission with lower latency connecting cities, countries, and continents. The 800,000 miles (about 1,287,475 km) of underwater cables support 99% of the internet network and over USD 10 trillion in financial transactions. The control over this critical infrastructure can be leveraged for espionage, data manipulation, or interruption of communication services. Global fiber networks present complex security challenges that are a significant concern for governments and companies alike.

The Lifeline of the Internet

Both terrestrial and underwater cables are vulnerable to spying and sabotage as intercepting these data links can provide access to a treasure trove of information. The tapping of communications cables isn't a new phenomenon – it featured heavily in WWI and the Cold War; more recently, the Snowden revelations revealed details on how intelligence agencies tapped directly into fiber optic cables of the global communications infrastructure.

Cable networks pass through international territory making the legal jurisdiction ambiguous. Physical security is limited, and modern technological advances have made it feasible to tap into these cables without severing them. Specialized devices can be used to bend the fiber slightly and capture some of the light signals passing through without causing a noticeable drop in the signal. Both the US and UK government have warned about Russian and Chinese underwater activities directly threatening subsea cable systems.

Ownership and control of these networks are strategically important, for national telecommunications, international connectivity, and cyber security. These assets are typically considered critical infrastructure and are subject to regulation and protection by national governments. Due to the high investment, optical fiber cables are often leased. If a company controls a fiber optic network, it likely has the capability—or may even be compelled by national laws—to monitor the data transmitted over these networks. Various nations have laws that collectively create an environment in which private companies operating are legally obligated to cooperate with intelligence and security agencies.

The Underwater Battleground Defines US-China Rivalry

Due to the importance in global communications and data transfer, undersea cables play a significant role in the US-China strategic competition. China is increasingly involved in laying new cables, raising concerns about data security, surveillance, and potential conflicts over critical digital infrastructure.

In Spring 2023, it was reported that Chinese state-owned telecom firms are mapping out a $500 million undersea fiber-optic internet cable network — the world's most advanced and far-reaching subsea cable network that would connect Asia, the Middle East and Europe. China's HMN Technologies, formerly Huawei Marine Networks, will manufacture and lay the undersea network.

There continues to be deep concerns about how Chinese infrastructure may provide a backdoor for eavesdropping on sensitive communications, military secrets, and corporate IP. Many of China's largest companies are state-owned or state-affiliated, receiving guidance, subsidies, and support from the government. There is a particularly close relationship between Chinese tech companies and the Chinese government in the realm of data sharing and surveillance.

The Chinese government leverages its corporate sector as a tool for national security and global influence. Access to data transmitted across fiber networks is enshrined in Chinese law: China's Counter-Espionage Law (2014), Anti-Terrorism Law (2015), National Intelligence Law (2017) and Cybersecurity Law (2017) collectively mandate that telecommunications operators and internet service providers must cooperate with state security and intelligence efforts. This potentially includes providing access to data transmitted through their networks, jeopardizing confidentiality and integrity of the transmitted communications. Collectively, the Chinese legal framework has implications for both domestic and international operations, particularly for the security and privacy of data within China.

Arqit SKA Platform™: A Mitigating Strategy

The security threats of utilizing fiber optic networks are significant. Enhanced security measures can mitigate many of these risks. Implementing end-to-end encryption safeguards data integrity and confidentiality. Due to the critical nature of these networks, continuous authentication is essential to guard against emerging threats.

Arqit SKA Platform, a cybersecurity product creates split-trust quantum-safe symmetric encryption keys at endpoints to protect data in transit and data at rest. SKA Platform is a lightweight, cloud-based advanced encryption technology designed to meet the evolving needs of modern communication networks. Parties can exchange cryptographic keys over a public channel without any risk of interception or eavesdropping. This closes attack surfaces and provides robust remote key management. It can be easily integrated into today's existing complex networks with no specialized hardware. Arqit's SKA Platform is easy to consume and now integrated with Intel Xeon processors, Fortinet and Juniper firewalls and HPE Aruba 5G networks.

Arqit SKA Platform embodies "zero trust" - an approach that requires endpoints to be continuously authenticated:

- Any physical endpoint can be a keyable resource
- All communication is secured regardless of network location
- Access to enterprise resources is granted on a per-session basis with enforced continuous authentication of endpoints
- Access to resources is determined by dynamic policy
- Continuous enterprise monitoring and measurement of the integrity and security posture of all owned and associated assets

SKA Platform is interoperable with standards such as RFC8784 and TLS 1.3 and uses the globally de facto standard AES256. SKA Platform is resistant to future attacks from quantum computers, easy to implement, lightweight and offers remote key lifecycle management.

Arqit **won the top award** at the Annual Mobile World Congress 2024 in Barcelona run by the industry body GSMA, which published this **White Paper** on Arqit's technology for 5G.

Arqit is ISO27001 accredited.