Albritton Center
for Grand Strategy
THE BUSH SCHOOL • TEXAS A&M UNIVERSITY

2034 and the Threat of Russian Submarine Cable Sabotage

By: Lane Burdette

Submarine communications cables are critical infrastructure which carry over 97% of all internet traffic, including $10 trillion in global transactions. They are irreplaceable, as transmission via satellite is slower, more expensive, and insufficient to meet capacity needs even if dramatically improved. There are currently 426 publicly known, in-service submarine cables globally. Cable faults are common—more than 100 are reported annually—and most breaks are the result of normal finishing or anchoring activity. However, the submarine cable network is vulnerable to manipulation. Espionage operations are widespread and, in rare instances, connectivity may be intentionally sabotaged. Current international governance is insufficient to safeguard the global network in periods of conflict, in which even neutral states may be adversely affected, or to facilitate timely repairs. What legislation exists faces an implementation gap. Overall, submarine cables have been largely ignored, and the US lacks a cohesive strategy to ensure their security. As media, policy, and scholarly attention to the cable network increases—accelerated by strategic competition in information and cybersecurity—it is necessary to ground security debates in factual analysis.

After the Huawei Marine espionage scandal entered public discourse, the U.S. took steps to counter China's influence over the submarine cable network (see the now archived Clean Network Initiative and the Blue Dot Network). I discuss threats posed by China and the need for a coordinated US response in a recent Journal of Public and International Affairs article. The Russian threat is less clearly defined. A flurry of news articles emerged following publication of a 2015 New York Times piece which made Cold War comparisons on the basis of aggressive Russian submarine activity near cable routes, but some argue that the threat of sabotage has been inflated. Could potential Russian sabotage be another media myth, like the continued risk to submarine cables from shark bites?

Undoubtedly, Russia engages in a pattern of activity near submarine cables. Much of this is attributed to the Yantar, a Russian spy ship which hosts two undersea submersibles and is likely capable of cable tapping, cutting, and/or delousing (removing taps). The ship has a habit of disappearing in key areas and may be associated with a 2016 Syrian internet outage. Russia has also manipulated internet infrastructure before, albeit terrestrially, during its annexation of Crimea. Less is understood about Russia's intentions regarding the submarine cable network or the potential effects of sabotage. One of the loudest voices in this debate is Admiral James Stavridis, USN (Ret.), former Supreme Allied Commander at NATO. Stavridis is frequently quoted and has written several pieces on the Russian threat, including a 2016 Huffpost article and the preface for a 2017 UK think tank Policy Exchange report. His most recent publication is *2034*, a novel which imagines a fictional scenario for conflict in the South China Sea that escalates to and beyond Russian submarine cable sabotage in the Arctic.

Stavridis and co-author Elliot Ackerman posit that this act, which takes place in the Barents Sea and damages an unnamed number of cables (3+) using explosives, slows US internet connectivity by 60%. Fatally, the authors also list the presence of sharks as possible operational cover. Though the destruction of cables could negatively affect regional connectivity, there are few places (e.g., Egypt) where localized sabotage would dramatically affect US international connectivity given the state's high network redundancy. The Barents Sea is not one of them, as no in-service, public cable passes through the region. Though Arctic routing is expected to increase in coming years, only one planned project would pass through the Barents Sea, and it would not connect to the contiguous US. Regardless, even if every cable connecting to the contiguous US could be sabotaged, domestic communications would still be possible and the attack would pose a severe threat to Russia's own connectivity. *2034*'s characterization of Russian sabotage therefore stretches beyond imagination into impossibility and demonstrates how threats to submarine cables, so often legitimate, may be overstated.

It is important to advocate for improved awareness of submarine cable security issues and urge protection of global internet infrastructure. Novels like *2034* also play a key role in imagining and preventing future scenarios for conflict. However, Russian submarine cable sabotage is not a credible threat to internet connectivity within the contiguous US. A more nuanced understanding of threats posed by Russia is needed to formulate US cyber strategy which protects physical infrastructure alongside digital assets. Future work analyzing the threat of Russian sabotage to submarine cables should focus on the potential risk to the Department of Defense Information Network, Nordic states, or areas of coastal, post-Soviet states that lack redundant terrestrial alternatives.