The New York Times | http://nyti.ms/1KyD7Hl

EUROPE

Russian Ships Near Data Cables Are Too Close for U.S. Comfort

By **DAVID E. SANGER** and **ERIC SCHMITT** OCT. 25, 2015

WASHINGTON — Russian submarines and spy ships are aggressively operating near the vital undersea cables that carry almost all global Internet communications, raising concerns among some American military and intelligence officials that the Russians might be planning to attack those lines in times of tension or conflict.

The issue goes beyond old worries during the Cold War that the Russians would tap into the cables — a task American intelligence agencies also mastered decades ago. The alarm today is deeper: The ultimate Russian hack on the United States could involve severing the fiber-optic cables at some of their hardest-to-access locations to halt the instant communications on which the West's governments, economies and citizens have grown dependent.

While there is no evidence yet of any cable cutting, the concern is part of a growing wariness among senior American and allied military and intelligence officials over the accelerated activity by Russian armed forces around the globe. At the same time, the internal debate in Washington illustrates how the

United States is increasingly viewing every Russian move through a lens of deep distrust, reminiscent of relations during the Cold War.

Inside the Pentagon and the nation's spy agencies, the assessments of Russia's growing naval activities are highly classified and not publicly discussed in detail. American officials are secretive about what they are doing both to monitor the activity and to find ways to recover quickly if cables are cut. But more than a dozen officials confirmed in broad terms that it had become the source of significant attention in the Pentagon.

"I'm worried every day about what the Russians may be doing," said Rear Adm. Frederick J. Roegge, commander of the Navy's submarine fleet in the Pacific, who would not answer questions about possible Russian plans for cutting the undersea cables.

Cmdr. William Marks, a Navy spokesman in Washington, said: "It would be a concern to hear any country was tampering with communication cables; however, due to the classified nature of submarine operations, we do not discuss specifics."

In private, however, commanders and intelligence officials are far more direct. They report that from the North Sea to Northeast Asia and even in waters closer to American shores, they are monitoring significantly increased Russian activity along the known routes of the cables, which carry the lifeblood of global electronic communications and commerce.

Just last month, the Russian spy ship Yantar, equipped with two self-propelled deep-sea submersible craft, cruised slowly off the East Coast of the United States on its way to Cuba — where one major cable lands near the American naval station at Guantánamo Bay. It was monitored constantly by American spy satellites, ships and planes. Navy officials said the Yantar and the submersible vehicles it can drop off its decks have the capability to cut cables miles down in the sea.

“The level of activity,” a senior European diplomat said, “is comparable to what we saw in the Cold War.”

One NATO ally, Norway, is so concerned that it has asked its neighbors for aid in tracking Russian submarines.

Adm. James Stavridis, formerly NATO’s top military commander and now dean of the Fletcher School of Law and Diplomacy, said in an email last week that “this is yet another example of a highly assertive and aggressive regime seemingly reaching backwards for the tools of the Cold War, albeit with a high degree of technical improvement.”

The operations are consistent with Russia’s expanding military operations into places like Crimea, eastern Ukraine and Syria, where President Vladimir V. Putin has sought to demonstrate a much longer reach for Russian ground, air and naval forces.

“The risk here is that any country could cause damage to the system and do it in a way that is completely covert, without having a warship with a cable-cutting equipment right in the area,” said Michael Sechrist, a former project manager for a Harvard-M.I.T. research project funded in part by the Defense Department.

“Cables get cut all the time — by anchors that are dragged, by natural disasters,” said Mr. Sechrist, who published a study in 2012 of the vulnerabilities of the undersea cable network. But most of those cuts take place within a few miles from shore, and can be repaired in a matter of days.

What worries Pentagon planners most is that the Russians appear to be looking for vulnerabilities at much greater depths, where the cables are hard to monitor and breaks are hard to find and repair.

Mr. Sechrist noted that the locations of the cables are hardly secret. “Undersea cables tend to follow the similar path since they were laid in the

1860s," he said, because the operators of the cables want to put them in familiar environments under longstanding agreements.

The exceptions are special cables, with secret locations, that have been commissioned by the United States for military operations; they do not show up on widely available maps, and it is possible the Russians are hunting for those, officials said.

The role of the cables is more important than ever before. They carry global business worth more than $10 trillion a day, including from financial institutions that settle transactions on them every second. Any significant disruption would cut the flow of capital. The cables also carry more than 95 percent of daily communications.

So important are undersea cables that the Department of Homeland Security lists their landing areas — mostly around New York, Miami and Los Angeles — at the top of its list of "critical infrastructure."

Attention to underwater cables is not new. In October 1971, the American submarine Halibut entered the Sea of Okhotsk north of Japan, found a telecommunications cable used by Soviet nuclear forces, and succeeded in tapping its secrets. The mission, code-named Ivy Bells, was so secret that a vast majority of the submarine's sailors had no idea what they had accomplished. The success led to a concealed world of cable tapping.

And a decade ago, the United States Navy launched the submarine Jimmy Carter, which intelligence analysts say is able to tap undersea cables and eavesdrop on communications flowing through them.

Submarines are not the only vessels that are snooping on the undersea cables. American officials closely monitor the Yantar, which Russian officials insist is an oceanographic ship with no ties to espionage.

"The Yantar is equipped with a unique onboard scientific research

complex which enables it to collect data on the ocean environment, both in motion and on hold. There are no similar complexes anywhere," said Alexei Burilichev, the head of the deepwater research department at the Russian Defense Ministry, according to sputniknews.com in May 2015.

American concern over cable cutting is just one aspect of Russia's modernizing Navy that has drawn new scrutiny.

Adm. Mark Ferguson, commander of American naval forces in Europe, speaking in Washington this month said that the proficiency and operational tempo of the Russian submarine force was increasing.

Citing public remarks by the Russian Navy chief, Adm. Viktor Chirkov, Admiral Ferguson said the intensity of Russian submarine patrols had risen by almost 50 percent over the last year. Russia has increased its operating tempo to levels not seen in over a decade. Russian Arctic bases and their $2.4 billion investment in the Black Sea Fleet expansion by 2020 demonstrate their commitment to develop their military infrastructure on the flanks, he said.

Russia is also building an undersea unmanned drone capable of carrying a small, tactical nuclear weapon to use against harbors or coastal areas, American military and intelligence analysts said.

Admiral Ferguson said that as part of Russia's emerging doctrine of so-called hybrid warfare, it is increasingly using a mix of conventional force, Special Operations mission and new weapons in the 21st-century battlefield.

"This involves the use of space, cyber, information warfare and hybrid warfare designed to cripple the decision-making cycle of the alliance," Admiral Ferguson said, referring to NATO. "At sea, their focus is disrupting decision cycles."

A version of this article appears in print on October 26, 2015, on page A1 of the New York edition with the headline: Russian Ships Near Data Cables Are Too Close for U.S. Comfort.