Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

Nation-State Research Activities as a Deniable Cover for Espionage

June 2022

INTENT

This white paper is designed to provide analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject.

Nation-State Research Activities as a Deniable Cover for Espionage

Introduction

For decades, foreign nation-states have conducted scientific research activities suspected of being used as cover for espionage objectives. Many platforms and sensors utilized for scientific research can be dual-use in nature, providing deniable cover for espionage. Moreover, many vessels utilized for military or intelligence purposes can be designated as research/scientific in order to avoid scrutiny from foreign governments and/or the general public. This paper will examine the background of such scientific research activities, as well as the potential for them to be deniable cover for espionage. A series of case studies involving U.S. adversaries such as Russia and China will also be presented.

Background

Data gathering is a common element of scientific research. The type, quantity, and quality of the data gathered varies by the tools used. State-funded scientific research is common, spanning numerous academic fields. However, this norm can also be capitalized on by state intelligence services. Using plausible research goals as cover, maritime vessels, satellites, aircraft and other vehicles/platforms can gather covert data with the goal of uncovering information about other nations. Various forms of mapping and geographical surveillance could uncover hidden assets and patterns in targeted countries. Scientific research projects could also serve as cover for testing new military or intelligence tools.

As with any discussion of espionage tools and tactics, much of the discussion must remain speculative, as open source information access is limited. Additionally, it is worth noting that the case studies in this white paper have a naval focus due to the amount of publicly available data about such activities. Academics may use topographical and geographical data for scientific studies and advancement. Oceanographic mapping is permitted by international law in many areas. However, the gathering of this mapping data may also result in insights benefitting malicious actors. Mapping data may also include the locations of underwater cables, sunken naval assets, or active crafts.[1,2] It should be noted that other tools (whether air- or ground-based) may serve as vessels of concern for espionage activity (including aircraft, satellites, ground vehicles, and remote ground-based sensors).

There is a great deal of history regarding these dual-use technologies. For example, when the first US space shuttles were revealed in the 1970s, Soviet leader Leonid Brezhnev believed that these were tools for releasing bombs from space, rather than academic exploratory vessels.[3] Conversely, spy satellites from the 1960s and 1970s gathered images now used by climate scientists to track decades of changes around the world, from the movement of glaciers to the erosion of shorelines. This highlights the overlap between the type of data scientists and intelligence groups may seek to gather.[4]

Case Study: Russian Vessel Yantar

The Russian oceanographic research vessel Yantar was launched in May 2015 after approximately five (5) years of construction and trials. The vessel is 354 feet long, it can travel 15 knots per hour, and it is manned by a crew of 60 sailors. The vessel is also equipped with two self-propelled deep submergence vehicles.[5] The Yantar belongs to Russia's Main Directorate of Underwater Research, which is part of its Defense Ministry. Russia maintains its official position that the vessel is purely for scientific research. However, the Yantar's function as a "spy ship" is less of an open secret than it is a near-universally agreed-upon fact. The vessel has been suspected of floating in the vicinity of the undersea Submarine Communications Cables (SCC), which carry internet traffic and military communications under the ocean.

Because the Yantar is officially a research vessel, she broadcasts her position on AIS. However, open sources in both the government and the media continue to allege that the Yantar's purpose is to tap or bug SCCs when its AIS is off. Officially, it has yet to do so. However, the Yantar has been seen conducting operations off Syria, in the Persian Gulf, and near Naval Submarine Base Kings Bay, Georgia in August 2015. It has also been sighted off the coast of Ireland near Trans-Atlantic internet cables in August 2021.[6,7,8] The Yantar's last official position was broadcast on 15 October 2021 in the Skagerrak strait en route to the port city of Murmansk, Russia via the Baltic Sea. She was estimated to arrive on 30 October 2021, but open sources have no official confirmation of the vessel reaching port.[9] Open source (but unverified) analysis asserts that the Yantar left her base in Olenya Guba near the Kola Peninsula in Northern Russia in March 2022.[10]

Case Study: Chinese Vessel Xiang Yang Hong 01

The Chinese research vessel Xiang Yang Hong 01 was commissioned in 2016 and is a vessel in the Chinese research segment that is believed to be involved in intelligence collection services for the Chinese military. The vessel is a member of a class of Chinese oceanographic survey and research vessels that were among China's first ocean survey vessels. China currently possesses around 60 oceanographic survey vessels that are in use. The Xiang Yang Hong 01 is a vessel capable of performing marine environmental element detection, marine surveys, and measurements of specific ocean parameters. As science and technology has developed over recent years, China's oceanographic survey vessels such as the Xiang Yang Hong 01 have seen ocean measurement expand from single water depth measurement to seabed topography, marine meteorology, ocean hydrology, etc. Furthermore, geographical characteristics have been embedded in vessels such as space remote sensing and polar parameter measurement.

In January and February of 2020, the Xiang Yang Hong 01 was detected mapping waters and conducting deep water surveys in the Indian Ocean off the Western Australian Coast where submarines are known to regularly transit. During the same timeframe in which the Xiang Yang Hong 01 was detected off the Western Coast of Australia, the Virginia-class fast-attack submarine USS Texas arrived at HMAS Stirling Naval Base for a port visit on the Western Coast of Australia. The Xiang Yang Hong 01 has a history of surveilling waters in the Pacific region as seen in 2018 where the vessel was found to be operating illegally within the Exclusive Economic Zone of Palau. The Australian Border Force (ABF), the Department of Home Affairs, and Australia's Department of Defence is well aware of Xiang Yang Hong 01's operations and has noted China's mission to map waters used by Australian submarines heading to and from the South China Sea. Although the Xiang Yang Hong 01 has stayed within international waters and has not entered the Australian Exclusive Economic Zone (AEEZ) unlawfully, Chinese oceanographic research vessels and the surveys they conduct in the western Pacific could potentially stimulate maritime conflict with U.S. operations in the region as this rapidly expanding oceanographic research vessel fleet continues to develop and collect research for intelligence and military purposes.

China's maritime activity, specifically in the Indo-Pacific region, is a situation to be monitored going forward as China continues to "leverage military modernization, influence operations, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to their advantage". Furthermore, it is probable that China will continue its economic and military ascendence by asserting power in the region and continue to "pursue a military modernization program that seeks Indo-Pacific regional hegemony in the near-term and displacement of the U.S. to achieve global preeminence in the future."[11,12,13,14]

Case Study: China Acoustic Sensors Near Guam

In December 2017, open source reports indicated that Chinese scientists had been found lowering acoustic sensors at the bottom of the Pacific Ocean in the Mariana Trench. These acoustic sensors have the capability to pick up acoustic signatures more than 620 miles away. Acoustic sensing is a key component of ocean observation and can be used to study oceans as well as to track submarines. The acoustic sensors have been placed near the U.S. territory of Guam which is home to Naval Base Guam. This technology can be found approximately seven (7) miles below the ocean's surface, which is at the Pacific's deepest location in the Mariana Trench.

China has been testing and placing acoustic sensors along its coastline for about ten years as the country continues to rapidly develop its oceanography and surveillance capabilities in an attempt to close the technological gap with adversaries such as the U.S. Navy. Although these devices have been ostensibly placed for scientific and research purposes, acoustic sensors have been reported to have the capability to potentially track U.S. and other foreign submarines IVO Naval Base Guam and surrounding regions within the western Pacific. Additionally, such sensors could potentially intercept the submarines' communications.

The strategic placement of these devices has raised questions regarding whether this technology is merely for research purposes, or whether the acoustic sensors are being used for intelligence gathering. The U.S. Navy has developed submarines that are able to effectively avoid detection, gather intelligence, and provide a strong deterrent to foreign adversaries and militaries such as China. Should open source findings and reports of Chinese surveillance technology being used as intelligence tools that have the ability to monitor underwater communications transmissions and any other acoustic communications be an accurate assessment, foreign adversaries to China are likely to have their military movement and activity restricted across the South China Sea with increased surveillance techniques and capabilities.[15,16]

Outlook

Foreign nation-states will almost certainly continue to utilize deniable scientific and research programs/equipment in order to support their own espionage objectives. Such activities allow espionage to "hide in plain sight" under the guise of legitimate scientific, research, or mapmaking programs. The information gleaned from such efforts likely supports military objectives, particularly naval objectives which rely on an understanding of oceanography. While much of this information is difficult to obtain through open sources, RMC's Intelligence & Analysis Division continues to monitor any available information regarding such activities by U.S. adversaries worldwide.

[1] *Ocean Mapping for Article 76*. (2021, October 5). Hydro International. https://www.hydro-international.com/content/article/ocean-mapping-for-article-76

[2] US Department of Commerce, NOAA, National Oceanic and Atmospheric Administration. (n.d.). *Law of the Sea*. NOAA Office of General Counsel International Section. https://www.gc.noaa.gov/gcil_law_sea.html

[3] Bodner, M. (2015, January 29). *Top 3 Successes of Soviet Economic Espionage*. The Moscow Times. https://www.themoscowtimes.com/2015/01/29/top-3-successes-of-soviet-economic-espionage-a43360

[4] Sanchez, K. (2021, January 5). *Go read these stories about the use of spy satellite images in environmental studies*. The Verge. https://www.theverge.com/2021/1/5/22215778/spy-satellites-cia-climate-change-environmental-studies-new-york-times

[5] GlobalSecurity.org. (2019, February 12). Project 22010 Kruys / Yantar Oceanographic Research Vessel. Retrieved June 10, 2022, from https://www.globalsecurity.org/military/world/russia/22010.htm#selection-677.189-677.496.

[6] Sutton, H.I. (2019, November 10). Russia's Suspected Internet Cable Spy Ship Appears Off Americas. Retrieved June 10, 2022, from https://www.forbes.com/sites/hisutton/2019/11/10/russias-suspected-internet-cable-spy-ship-appears-off-americas/?sh=3506945142d5.

[7] Peter, L. (2018, January 3). What Makes Russia's New Spy Ship Yantar Special? Retrieved June 10, 2022, from https://www.bbc.com/news/world-europe-42543712.

[8] Sutton, H.I. (2021, August 19). Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables. Retrieved June 10, 2022, from https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/.

[9] MarineTraffic. (2021, October 15). Yantar – Latest Position. Retrieved June 10, 2022, from https://www.marinetraffic.com/en/ais/details/ships/shipid:1215053/mmsi:273546520/imo:7524419/vessel:YANTAR.

[10] Sutton, H.I. (2022, March 6). Controversial Russian Spy Ship Yantar Leaves Base. Retrieved June 10, 2022, from http://www.hisutton.com/Russian-Spy-Ship-Yantar-2022-03-06.html.

[11] (U) Greene, A. (2020, March 1). Chinese Research Vessel Xiang Yang Hong 01 Tracked in Waters Near Christmas Island off Western Australia. Retrieved June 10, 2022, from https://www.abc.net.au/news/2020-03-02/chinese-research-vessel-tracked-defence-subs-western-australia/12009708.

[12] (U) Global Security. (n.d.0). Xiang Yang Hong (AGOR/AGI). Retrieved June 10, 2022, from https://www.globalsecurity.org/military/world/china/xyh.htm.

[13] (U) CSIS. (2020, April 16). A Survey of Marine Research Vessels in the Indo-Pacific. Retrieved June 10, 2022, from https://amti.csis.org/a-survey-of-marine-research-vessels-in-the-indo-pacific/.

[14] (U) Garamone, J., DOD News. (2020, June 5). White House Report Recommends Multi-Pronged Approach to Counter China. Retrieved June 10, 2022, from https://www.defense.gov/News/News-Stories/Article/Article/2210283/white-house-report-recommends-multi-pronged-approach-to-counter-china/.

[15] (U) Kuhn, A. (2018, February 6). China is Placing Underwater Sensors in the Pacific Near Guam. Retrieved June 10, 2022, from https://www.npr.org/sections/parallels/2018/02/06/582390143/china-is-placing-underwater-sensors-in-the-pacific-near-guam.

[16] (U) Trevithick, J. (2019, June 30). China Reveals it has Two Underwater Listening Devices Within Range of Guam. Retrieved June 10, 2022, from https://www.thedrive.com/the-war-zone/17903/china-reveals-it-has-two-underwater-listening-devices-within-range-of-guam.