Umanets, M., 2024. *Geopolitical dimensions of the Houthi interference with submarine cable communications in the Red Sea,* Przegląd Geopolityczny, 50, s. 51-67.

Mariia UMANETS
National Radioelectronics Univ. of Kharkiv, Ukraine
ORCID: 0000-0003-4459-2346

GEOPOLITICAL DIMENSIONS OF THE HOUTHI INTERFERENCE WITH SUBMARINE CABLE COMMUNICATIONS IN THE RED SEA

GEOPOLITYCZNE UWARUNKOWANIA INGERENCJI HUTICH W PODMORSKĄ KOMUNIKACJĘ KABLOWĄ NA MORZU CZERWONYM

Abstract

The paper examines the possible intentional damage of 3 submarine cables in the Red Sea by the Yemeni Houthis. It considers the history of Yemen's civil war, political and rebel views, potential allies of the Houthis, military arsenal, and motives. This topic is more relevant than ever for several reasons. Firstly, the security of undersea telecommunications infrastructure is critical to ensuring uninterrupted global Internet traffic and data exchange. Secondly, the active escalation of the Israeli-Arab conflict and the Houthi attacks on shipping in the Red Sea make serious risks and possible incidents that can lead not only to significant economic losses but also to geopolitical instability.

For a detailed analysis, research studies and articles related to the Yemeni civil war, Iran's involvement and support, and the provision of the necessary military resources for attacks on land and sea, as well as the physical structure of the submarine cables were examined. The paper analyzes in detail the incident, and the methods and means that could have been used to carry out such an operation. The economic and political consequences of repeated and more serious damage to submarine cables are assessed. The problem described in the paper is important to prevent the highly probable sabotage of the submarine fiber optic cable network and to better understand the consequences.

Keywords: Houthis, undersea cables, Yemen, Iran, submarine.

Introduction

The importance of undersea cable infrastructure (SCI) cannot be underestimated. Over 99% of all Internet traffic passes through SCI, which has a total length of 1.4 million kilometers (Mauldin 2023). Any

damage to SCI would have significant consequences for global communication, potentially slowing down the Internet. If the scale and geography of the damage increases, the consequences could include disruption of e-commerce and financial markets, as well as limiting public access to information and vulnerability of informational infrastructure. It is important to note that this list could become extremely long.

According to TeleGeography, more than half of the inter-regional bandwidth of many countries is connected to Europe via Red Sea cables. Additionally, cables in the Red Sea carry over 90% of all bandwidth between Europe and Asia.

Recent news has been related to the Iranian-backed Houthi rebels who have intervened in the conflict between Israel and Hamas. Their actions, including boarding, rocket attacks, and the use of drones, have effectively stopped shipments through the Suez Canal and the Red Sea. The Bab el-Mandeb Strait, which is about 29 km wide at its narrowest point, is where the raids take place.

In February 2024, several undersea communication cables running through the Red Sea were reported as cut, resulting in a decrease of at least 25% in traffic between Asia and Europe, according to HGC Global Communications, Hong Kong's internet provider. The affected cables were SEACOM/Tata TGN-Eurasia, Asia-Africa-Europe 1, and Europe India Gateway. Seacom, an African telecommunications cable operator, reported that initial testing indicated that the affected segment was within Yemeni maritime jurisdiction in the southern Red Sea. Before the incident, Yemen's legitimate, UN-recognized government in Aden had warned that the Houthis were threatening to sabotage important undersea communication cables[1],, including internet lines that run along the bottom of the Red Sea, connecting Asia to Europe. The warning was issued after a Houthi-affiliated channel on the Telegram messenger published a map displaying undersea cable routes in the Red Sea[2],. This paper will provide a detailed analysis of the event, including its various aspects, causes, opportunities, and consequences, as well as possible scenarios for future developments.

[1] Republic of Yemen Ministry of Foreign Affairs and Expatriates website: https://www.mofa-ye.org/Pages/25833/, (accessed on 01 Apr. 2024)
[2] MEMRI's Jihad and Terrorism Threat Monitor (JTTM) Report: https://www.memri.org/jttm/veiled-threat-telegram-channels-linked-houthi-ansar-allah-movement-point-submarine-internet#_edn1, (accessed on 01 Apr. 2024)

The history of the Houthis within the Yemeni Civil War

The starting point of almost every conflict in the Middle East is historical and religious contradictions, and to begin a detailed analysis and understand the motives of possible attacks on undersea telecommunications infrastructure in the Red Sea, it is necessary to review the historical context of the emergence of the Houthi movement, as well as the civil war in Yemen.

Houthi is a religious and political movement, and alleged paramilitary group, of Shiite tribes from the northern regions of Yemen. The group's members are primarily Zaidites, an offshoot of Shiism, and they make up 35-45% of the population in the northern regions of Yemen (Bryjka, 2016). The conflict in Yemen has its roots in the unification of the country in 1990, which failed to create a strong political unity due to economic and sociopolitical disparities, clan structures, and religious differences between the north and south. The situation has been further destabilized by the growing political radicalization of the Shiite Ansar Allah movement, which is centered around the influential Houthi family in the north and the activity of al-Qaeda in the southeast. In 2014, former President Ali Saleh made an alliance with the Houthis, dissatisfied with the new government, which led to a new uprising. Consequently, the Houthis rapidly gained the support of many military units, resulting in the division of the country into a pro-Shiite north and a pro-Sunni south. The active and politically charged scenario in Yemen is also related to the influence of external factors, the most important of which is the involvement of Yemen's internal political contradictions in the global conflict between Shiites and Sunnis, which is used by rival regional powers - Iran and Saudi Arabia (Otlowski, 2015).

The current political situation in Yemen shows that Iran's efforts have been better than Saudi Arabia's, not only because Iranian tactical support in the military operations has been significant, but also because the Houthi leadership has been given more autonomy by Tehran than the Yemeni government, which had relations with Riyadh. By granting more autonomy to the Houthis and following through with policies and rhetoric to that effect, the Iranian government managed to become a truly legitimate partner for the Houthis, while Saudi Arabia dictated the day-to-day governance of the Yemeni government, even at the local level. On November 19, 2019, the Iranian government officially handed over the Yemeni embassy in Tehran to the Houthis. In an effort to demonstrate their loyalty to Iran, Houthi representatives met with both

Hamas's external patrons and Iranian officials, and a spokesman for the Houthi forces testified to the readiness of the Houthi military to respond to potential Israeli threats (Kaussler, Grant, 2022).

Thus, one of the methods of expressing support for Hamas [3] in the current Israeli-Palestinian conflict is to attack ships, and now probably to sabotage undersea cables to destabilize telecommunications. According to the Congressional Research Service[4], since October 17, 2023, the Houthis have attacked commercial and military vessels more than 60 times. The threats are forcing many companies to divert ships from the Red Sea to a longer and more expensive voyage around Africa, disrupting global trade and causing significant economic losses.

On February 4, 2024, Yemen's General Telecommunications Company, which is affiliated with the UN-recognized government, issued a statement the Houthis' "threats to target international marine cables" [5]. A month later, in March 2024, it was announced that 3 undersea cables had been damaged and the Houthis of their own categorically denied any involvement in the incident in a press release issued on February 27, 2024. [6]

In the following, this study will analyze what opportunities and resources exist to carry out the planned sabotage of undersea cables, and whether the Houthis had such an opportunity. This requires an understanding of how undersea cables are deployed and the equipment needed to damage them.

Submarine cable structure

It is valuable to have a basic understanding of how undersea cables are constructed so that we can assess the likelihood of damage using the appropriate equipment, as most disruptions to submarine infrastructure are caused by unintentional human activity and natural

[3] Palestinian (Sunni) terrorist (recognized by Israel, Canada, the United States, Japan, the European Union, the Organization of American States, etc.) political and military organization governing the Gaza Strip.

[4] Christopher M. Blanchard, *Houthi Attacks in the Red Sea: Issues for Congress*. Available online:https://crsreports.congress.gov/product/pdf/IN/IN12301, (accessed on 01 Apr. 2024)

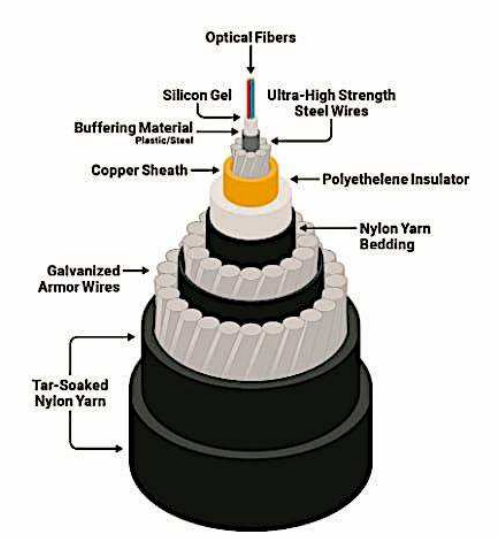
[5] Press Release Telecommunications Corporation and TeleYemen condemn Houthi militia's threats to target submarine cables. Available online: https://www.mofa-ye.org/Pages/25833/, (accessed on 01 Apr. 2024)

[6] Press Release on Red Sea Submarine Cables Incident. Republic of Yemen Ministry of Telecommunications and Information Technology. Available online: https://twitter.com/mtityemen/status/1762453092442706385, (accessed on 01 Apr. 2024)

disasters[7]. As stated by Stephen Drew (2009, p. 43-45) when an undersea cable suffers damage that affects data transmission, it is considered a fault.

The thickness of undersea cables varies depending on whether they are laid deep in the ocean or closer to shore. In the former case, the cable is typically as wide as a garden hose, and the fibers that carry the light signals are extremely thin - about the diameter of a human hair; those laid closer to shore have additional layers of armor for increased protection[3] (Fig. 1).

Fig. 1. Parts of an undersea cable



Source: Telegeography, '*Submarine Cable 101*' (see footnote 7).

When the cable is completely severed, both the optical fibers that transmit information and the copper conductor that carries the electrical current needed to power the signal amplifying repeaters used in long-range cable systems are damaged. The modern undersea telecommunications cable typically has an outer diameter ranging from approximately 17 to 50 millimeters, depending on the specific type of cable and its protective armor. These cables possess breaking strengths that vary from a few metric tonnes to over 40 tonnes for the double-armored variants. It should be noted, however, that despite its robust

[7] Telegeography, '*Submarine Cable 101*'. Available online: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions (accessed on 01 Apr. 2024)

design, the cable may fail under the influence of forces less than those required to break it completely. When a solid object comes into contact with a cable and penetrates its protective layers and insulation, the copper conductor responsible for carrying the electrical current is exposed. In such cases, the electrical current usually flows into the surrounding seawater, resulting in what is known as "shunting". However, the optical fibers inside the cable may remain intact and able to transmit signals. At the same time, however, the repeaters behind the shunt may lose power, causing the cable to fail. In some cases, it may be possible to equalize the voltage being transmitted to the electrical equipment at both ends of the cable, allowing the repeaters on either side of the shunt to continue operating temporarily, keeping the cable operational until the repair ship arrives (Drew, 2009).

Modes of attack on undersea cables

In recent years, NATO and European Union officials have increasingly focused on possible sabotage operations. One potential method is to arm civilian vessels, including research, fishing, and transport vessels, and use improvised explosive devices (IEDs) such as anchors and dredges. These forms of attack do not require technologically sophisticated capabilities, such as underwater capabilities, and are easy to carry out because vessels can be hidden in normal maritime traffic (Bueger, Liebetrau, Franken, 2022).

An example of the possible use of a research vessel for such purposes is the Russian ship “Yantar”[8], which has been spotted since 2015 near undersea cables off the coasts of Cyprus, Israel, Syria, Iran, and Ireland. In some cases, the ship's activities have coincided with temporary communications disruptions in neighboring countries, raising concerns among security and defense policymakers (Koka, 2022).

Another form of attack is the use of submersible boats, crafts, or military-grade drones and submarines, which can be manned or unmanned. However, the latest naval technology and advanced capabilities are not the ultimate means of sabotaging cables; there are less expensive means such as naval mines, maritime improvised explosive devices (MIEDs), low-profile submersible vessels, and even divers (Bueger, Liebetrau, Franken, 2022).

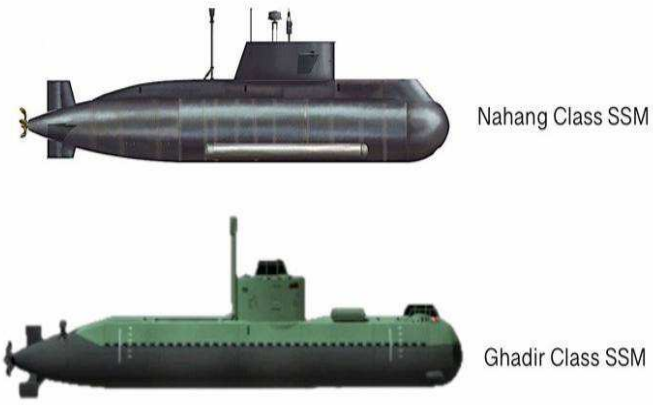
[8] The ship is designed to explore the world's oceans and seabed. For this purpose, the ship has special deep-sea manned and autonomous unmanned submersibles that can dive to a depth of about 6,000 meters. *Yantar* has been reported in position near undersea telecommunications cables.

Disruption of the cables could also be a side-effect of Iran's mine war. Tehran has already used sea mines in the Persian Gulf to disable cargo ships and oil tankers, and later the Yemeni Houthis used this tactic in the Red Sea. An attack on the network in choke points such as the Strait of Hormuz and Bab el-Mandeb poses a greater risk to multiple cables (Koka, 2022)

Based on data provided in the Defense Intelligence Agency's "*Iran Military Power*" report, Iran has two independent naval forces - the Islamic Republic of Iran Navy (IRIN), the naval branch of the Artesh, which has large and aging high-end capabilities, and the IRGCN, which has capabilities that meet the needs of low-cost strikes. Another report, *Iran: Enabling Houthi Attacks Across Middle East* contains a comparative analysis of publicly available images of Iranian missiles and UAVs with the ones displayed and used by the Houthi forces in Yemen for midget submarines may have been in the Houthis' possession, enabling them to effectively carry out their threats.

Potential submarines could be the 200-ton Ghadir submarine (capable of carrying two 533-millimeter torpedoes, or the 500-ton Nahang-class submarines (Fig. 2) operated by the IRGC and IRIN. These submarines are probably intended for mine-laying, special operations, and anti-shipping operations, and are indicative of Iran’s growing interest in developing an undersea warfare capability (Haghshenass, 2008).

Fig. 2. Nahang Class SSM and Ghadir Class SSM



Source: World Submarines: Covert Shores Recognition Guide (Sutton, Davis, 2017)

Geopolitical value of submarine cables

States increasingly consider international cables in national maritime zones to be critical infrastructure that deserves robust protection. Submarine fiber-optic cable networks carry approximately 95 percent of international communications and data traffic. In turn, the data carried by these cables plays an important role in the functioning of every country's critical industries: financial services, energy, health care, defense, global communications, and many others.

During a lecture for Harvard University, DeepMacro co-founder and managing director James Covey said: "*Everything you read about geopolitics, about spheres of influence and national interests and so forth has a counterpoint on the Internet and how Internet structure plays out*"[9]. To highlight the geopolitical importance of cables, consider the examples Covey used in his lecture.

The first one is Israel - a country surrounded by states with which it has had serious political conflicts for many years. The undersea cables that connect Israel to Europe and the United States run mostly through Cyprus, Greece, and Sicily. For the territory of Palestine, on the other hand, the connection is provided from two sides. Partly from Israel, but also from European operators whose traffic passes through Jordan, mainly via the FLAG Europe-Asia (FEA) cable. This cable also passes through Saudi Arabia with landing points in Dubba and Jeddah.

Turkey's geographically attractive position as a data bridge between Asia and Europe is extending its reach to its neighbors through investments in submarine cables to Iraq, the Caucasus and Saudi Arabia. The active involvement of telecommunications companies Turk Telecom International (TTI) and Turkcell Superonline (TSOL) has made Turkey a hub for connectivity to Europe. This shows that such an important thing as the provision of Internet, communication, data transmission can easily be used as an object of manipulation and as a way to increase influence over other countries and entire regions.

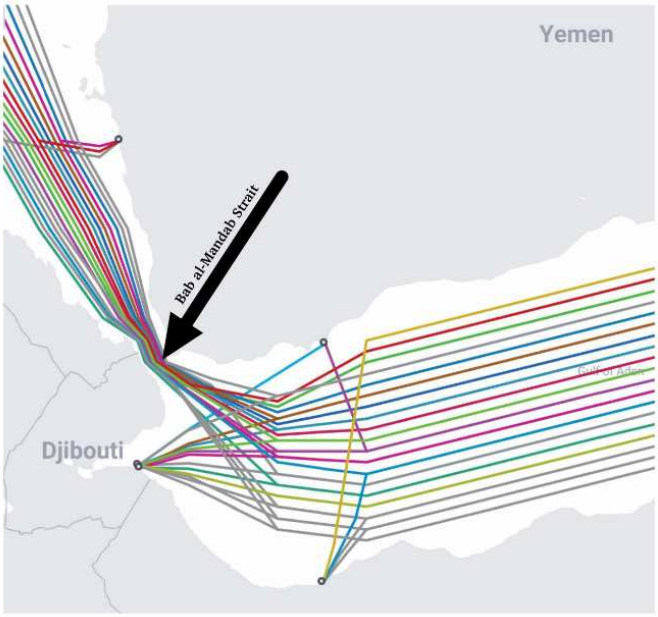
According to various reports, North Korea, Iran, Israel, and Turkey have employed "gray zone"[10] tactics in the maritime domain as part of militarized interstate disputes. Given that the coast of Yemen is

[9] A recording of James Covey's lecture held at the Berkman Center is available online: https://cyber.harvard.edu/events/luncheon/2011/11/cowie, (accessed: 04 Apr. 2024)

[10] The grey zone is defined as "competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality" by the United States Special Operations Command.

one of the main transmission routes of the Europe-Asia cable system (the concentration of cables can be seen in the figure), the war in Yemen and the role of the Houthis in international conflicts should be seen as a potential threat.

Fig. 3. Concentration of undersea cables in the Bab el - Mandeb Strait



Source: https://www.submarinecablemap.com/

The number of submarine cables around the world is growing due to the huge demand for data and cloud services. Moreover, the Europe, Middle East and Africa region (EMEA) is leading the way[11]. Therefore, it will be important to consider the risks for the European Union as well.

A complete blackout within the EU or one of its member states is unlikely, but when it comes to small naval bases, islands, the situation changes dramatically. For example, the western Indian Ocean is a region where extremist organizations are particularly active, as evidenced by maritime and land incidents in Djibouti, Mozambique, the Maldives, Somalia, Kenya, Sri Lanka, and Pakistan. This raises the possibility that attacks on submarine cables could be carried out to damage naval bases

[11] Subtel Forum Submarine Telecoms Industry Report, 2023-2024, Issue 12, pp. 36-37. Available online: https://subtelforum.com/industry-report/, (accessed on 12 Apr. 2024)

in Djibouti or Bahrain that are essential to ongoing naval operations in the region (e.g., the EU Naval Force Operation Atalanta or the European Maritime Awareness Strait of Hormuz operation (EMASOH)). In addition, the French overseas territories of Réunion and Mayotte could be at increased risk, not least because of poor connectivity (Bueger, Liebetrau, Franken, 2022, p. 33-34).

Control over submarine cable networks is an important lever of political influence. The location of cable hubs and routes can marginalize or increase the dependence of countries on the network. Submarine cables and their network structure are seen as a geopolitical tool and source of information, making them a key element in global surveillance and espionage systems. Geopolitical rivalries influence network expansion and the location of major Internet traffic exchange points (GIXs), increasing the influence of powers over certain regions and their dependence on them (Pèrez, 2023). States or terrorist organizations that have the resources and geographic advantage to destroy or compromise these nodes can also use them to support their political interests.

Analyzing the economic impact

The purpose of this section is to analyze the damage to the cables and examine the actual and potential economic losses. As mentioned earlier, in February 2024, parts of the following cable systems were damaged in the Red Sea:

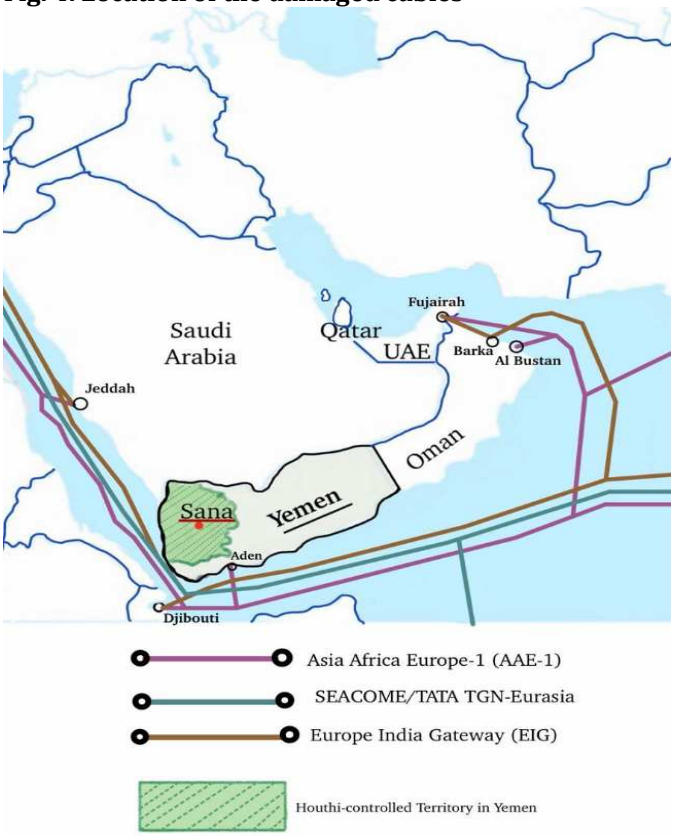
— SEACOM/Tata TGN-Eurasia: Cable Length15,000 km
— Asia Africa Europe-1 (AAE-1) Cable Length25,000 km
— Europe India Gateway (EIG) Cable Length15,000 km

All of these systems pass through the Bab el-Mandeb Strait, which connects the Red Sea to the Gulf of Aden in the Arabian Sea. The map below (Fig. 4) provides a closer look at the geography of the damaged cables and their concentration along the Yemeni Coast. Although the consequences of this attack were not critical, approximately 25% of Internet traffic in Asia, Europe, and the Middle East had to be rerouted to minimize customer disruption.

On March 5, 2024, user complaints about disruptions in the operation of social networks began to spread across the Internet. Andy Stone, a representative of Meta, confirmed the problems with the portals (Facebook, Instagram). Repairs to the damaged cables are also being hampered. Seacom's chief digital officer, Prenesh Padayachi, told CNN that repair work will not begin for at least a month, in part because of the lengthy time it takes to obtain work permits in the area. So what

economic losses could be caused by greater damage? During the research for this paper, an analysis was conducted to show how much a potential Internet outage would cost different countries over a given period of time. The NetLoss calculator[12]. was used to calculate FDI loss and GDP (PPP) loss for selected countries to visualize how restricting access to the Internet can affect a country's economic losses. The period chosen for the analysis is February 24, 2024 to March 10, 2024[13] (fig. 5).

Fig. 4. Location of the damaged cables

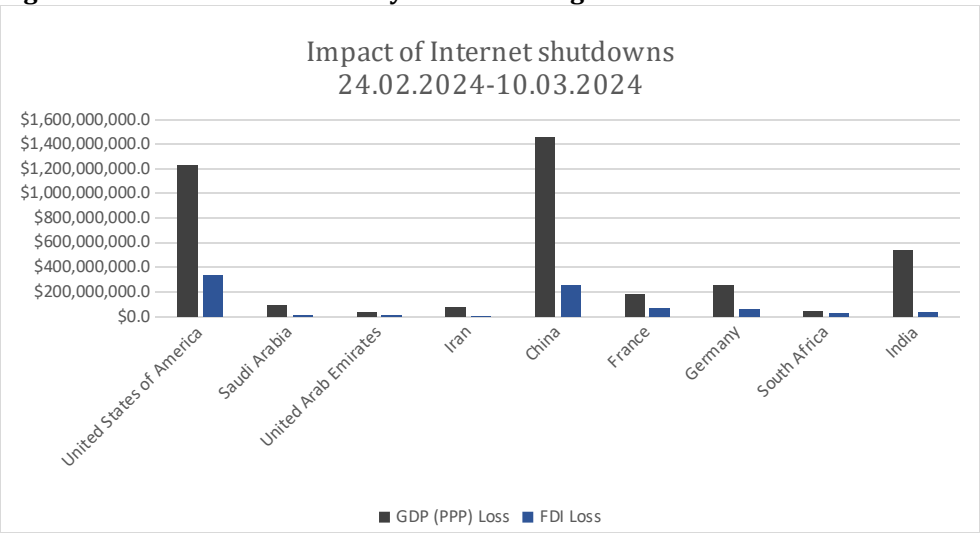


Source: own elaboration.

[12] The NetLoss_calculator is a tool that allows to estimate: The amount of Gross Domestic Product (GDP) lost during a shutdown, the amount of Foreign Direct Investment (FDI) lost due to a shutdown, and others. Available online: Netloss Calculator — Pulse (internetsociety.org) (accessed on 04 Apr 2024)

[13] The period was chosen precisely because it was the time when failures in the work of the Internet and various Internet resources were recorded.

Fig. 5. Economic losses caused by internet outages



Source: see footnotes 12 & 13.

As can be seen from the theoretical calculations above, serious Internet outages will cause significant economic losses. Consequently, keeping submarine cables running is essential to maintaining a stable global economy. The submarine cable infrastructure has made global financial services possible today. Any shutdown or major failure of the cable system would disrupt tens of millions of transactions. Every day, SWIFT transmits about 20 million messages to more than 8000 banking organizations, security institutions and corporate clients in almost 200 countries, ensuring the coordination of trillions of dollars worth of assets in the global financial markets (Martinage, 2015, p. 119), and now all this would not be possible without the use of submarine cables.

Submarine cable hacking and espionage

Manipulation and significant economic damage can play an important role in political confrontation, but the goal may not always be to damage or destroy a cable. In this section, we will look at methods of hacking undersea cables and examples of cable espionage for military purposes. Modern cables are fibre optic cables capable of carrying tens of terabytes of data per second. There are cables designed for military and intelligence purposes, but most carry commercial, private, and government information at the same time. Cable hacking requires specialized equipment such as submarines. As a result, most hacking is

likely to be carried out by governments (Griffiths, 2019). However, external groups are still considered a threat to undersea cables. Although it takes more sophisticated technology to hack a cable than to destroy it, the threat of terrorist hacking of submarine cables remains, even if it has not yet become a reality (Newman, 2020).

It is evident that the specifics of the methodology employed by the states are classified, yet a potential algorithm can be delineated. A submarine is utilized to execute such an operation, equipped with tools to sever cables. The "splicing method" penetrates the protective coating of the submarine cable and installs eavesdropping devices to collect transmitted data. This method has been challenged by experts due to the high probability that operators will swiftly detect a disruption in data transmission.

It is possible that other hacking methods may be less visible. Some analysts have suggested that operators access the cable at landing stations equipped with signal amplification and certain equipment to install intercept probes that pick up the fiber optic light signal and make a copy of it (Khazan, 2013). This method, and a similar one involving creating a slight curvature within the cable to siphon off data as it passes through the curve, may not alert an operator that hacking has occurred because the cable does not witness a service interruption seen in splicing. While these methods may result in some damage to the cable, they are not easily detected or defended against, even by states that are particularly vigilant.

In analyzing future threats, it is important to consider the military operations. Cases of cable espionage have been documented since the Cold War. In the 1970s, the United States began spying on Soviet cables as part of Operation Ivy Bells[14]. Using the Halibut submarine, the Americans installed a device that allowed them to read information on a cable in the Sea of Okhotsk. This cable connected the Soviet fleet base in Petropavlovsk-Kamchatsky to its headquarters in Vladivostok. Today, the US Navy – and certainly other navies as well – is able to intercept the data traffic routed through submarine fibre-optic cables (Heintschel von Heinegg, 2013). A prime example is the USS Jimmy Carter[15] that was put

[14] Operation Ivy Bells was a joint Cold War mission between the U.S. Navy, the CIA, and the NSA. The objective was to plant listening devices on Soviet undersea communication lines. The U.S. sought information on Soviet submarine and missile technology, including ICBM testing and nuclear first-strike capability.

[15] Nuclear-powered attack submarine that was commissioned in February 2005. It is just one of three Seawolf-class subs in service, but also the only one modified for Seabed

into service in 2005. This vessel is equipped with the capability to intercept transmitted messages via radio waves, a process referred to in military parlance as signals intelligence. The capacity to intercept data from undersea fiber-optic cables may be unique to the Navy. Jeffrey Richelson, an intelligence technology specialist, notes that in order to intercept fiber optic transmissions, intelligence operatives must physically place a listening device along the transmission route. In the event that the stations handling communications over the lines are located overseas or otherwise inaccessible, intercepting the line remains the only way to gain access to the data. It is claimed that the submarine also intercepts waves of fiber optic light by bending the cable slightly. While the amount of light that is emitted is negligible, it is sufficient to monitor the data traffic through the cable. The data from the transmission is then stored on board. It seems plausible to suggest that navies may also possess the capacity to launch cyberattacks via submarine cables and utilize them for a variety of military and operational purposes.

Potential future risks

Modern political conflicts never leave critical infrastructure unattended; it is always a key tool for pressure and manipulation. To underscore this point, consider the sabotage of the Nord Stream 2 pipelines in September 2022. The damage to the pipelines was found to be significant and could not have occurred naturally. The gas leak from the Nord Stream pipeline affected industry, the economy and the environment. Although the pipelines were not actively delivering gas, they were still holding it. The main consequences were the aggravation of the energy crisis in Europe, as the Nord Stream was one of the only ways to import Russian gas to Europe. The future security of other pipelines and energy sources is now in question and requires special monitoring. Europe will have to reduce its consumption of natural gas to cope with such a significant loss of supply (Mills, 2022). Investigations have not identified the ultimate perpetrator of the incident, but it was undoubtedly an opportunity to influence the conflict actors.

Consider now the similarities to the undersea cable situation which is the subject of this paper. The motives, historical background,

---

Warfare – those unreported missions deep below the waters that can target critical infrastructure such as power cables, telecom cables, and even natural resource extraction systems.

and economic implications are analyzed in the previous sections, as is the close relationship and direct impact on the Israeli-Palestinian conflict. Submarine cables, as well as submarine gas pipelines, are critical to the economy and the maintenance of various industrial sectors. This confirms once again that the sabotage of submarine cables in the Red Sea is no accident and cannot be ignored. This infrastructure is underwater and under the jurisdiction of different countries, which complicates the issue of security from a geopolitical point of view. The consequences of such sabotage are much more costly than its realization. Therefore, it is important to develop and implement the necessary strategies to secure undersea infrastructure at the right time, taking into account the geographical location and conditions of the facilities.

References

Bryjka, F., 2016. *Saudyjsko-irańska wojna zastępcza w Jemenie*, [w]: M. Bodziany (red.), *Społeczeństwo a wojna. Oblicza bezpieczeństwa w XX i XXI wieku*, WSO WL, Wrocław.

Bueger, C., Liebetrau, T., Franken, J., 2022. *Security threats to undersea communications cables and infrastructure – consequences for the EU*, European Parliament, Brussels.

Carter, L. et. al., 2009. *Submarine Cables and the Oceans – Connecting the World*. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC.

Drew, S., 2009. *Submarine cables and the oceans: connecting the world*, UNEP World Conservation Monitoring Centre, Cambridge.

Ganz, A., et. al., 2024. *Submarine Cables and the Risks to Digital Sovereignty*, Minds and Machines, 31 (3), s. 1-23.

Griffiths, J., 2019. *The Global Internet Is Powered by Vast Undersea Cables. But They're Vulnerable*, CNN. Available online: https://perma.cc/3VJM-LQQD (accessed 15 Apr. 2024)

Gugnin, A., Delong, M., Lisnevskaya, Y., 2021. *The problem of political leadership on the example of Yemen,* Przegląd Geopolityczny, 36, s. 98-109.

Haghshenass, F., 2008. *Iran's Asymmetric Naval Warfare*, Policy Focus, 87, pp. 13-16.

Heintschel von Heinegg W., 2013. *Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law, in Peacetime*

Regime for State Activities in Cyberspace, NATO CCD COE Publication.

Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance, 2019. DIA Report, pp. 48-76.

Karmon, E., 2017. *Yemen's Houthis: New Members of Iran's Anti-Israeli/Anti-American Axis*, ResearchGate. Available online: https://www.researchgate.net/publication/317345242 (accessed 15 Apr. 2024).

Kaussler, B., Grant, K.A., 2022. *Proxy War in Yemen*. Routledge Focus, New York.

Khazan, O., 2013. *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, The Atlantic. July 16. Available online: https://perma.cc/W8GY-F5R2 (accessed 15 Apr. 2024).

Knights, M., 2023. *An Heir and a Spare? How Yemen's "Southern Hezbollah" Could Change Iran's Deterrent Calculus*, The Washington Institute For Near East Policy Notes, 142, pp. 9-13.

Koka, A., 2022. *The Gulf Submarine Network amid Sabotage and Mine Warfare Threats*, The Euro-Gulf Information Centre (EGIC).

Kuoman, A., 2024. *Red Sea on edge: Houthi attacks disrupt vital shipping routes*, University of Navarra.

Martinage, R., 2015. *Under the Sea: The Vulnerability of the Commons*, Foreign Policy, 94, 1, pp.117-126.

Mauldin, A., 2023. *Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?* TeleGeography. Available online: https://blog.telegeography.com/2023-mythbusting-part-3 (accessed 15 Apr. 2024).

Mauldin, A., 2024. *The Red Sea: A Key Subsea Cable Crossroads Under Siege*, TeleGeography. Available online: https://blog.telegeography.com/the-red-sea-a-key-subsea-cable-crossroads-under-siege (accessed 15 Apr. 2024).

Mills, C., 2022. *Geopolitical implications of Nord Stream 2*, House of Commons Library, London.

Newman, L.H., 2020. *Cut Undersea Cable Plunges Yemen Into Days-Long Internet Outage*, Wired. Available online: https://perma.cc/C4AF-CLBG; (accessed 15 Apr. 2024).

Pérez, R.G., 2023. *Submarine Cables Across The Atlantic: Geopolitics and Security of a Critical Infrastructure*, Atlantic Center Report, 3, pp. 57-82.

Robinson, K., 2024. *Iran's Support of the Houthis: What to Know*, Council on Foreign Relations. Available online: https://www.cfr.org/in-brief/(accessed 15 Apr. 2024).

Saif, M., 2023. *Shades of grey: The evolving links CRU Policy Brief between the Houthi and Iran*, Netherlands Institute of International Relations.

Sechrist, M., 2012. *New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems*. Discussion Paper, Science, Technology, and Public Policy Program, Belfer Center.

Subtel Forum Submarine Telecoms Industry Report, 2023-2024, 12. Online: https://subtelforum.com/industry-report/, (accessed 12 Apr. 2024).

Threats To Undersea Cable Communications, 2017. TeleGeography, NASCA, IEEE, ICPC, CSRIC, CERT, ACMA.

Streszczenie

W artykule zbadano możliwe celowe uszkodzenie 3 kabli podmorskich na Morzu Czerwonym przez jemeńskich Hutich. Rozważono historię wojny domowej w Jemenie, stanowiska polityczne stron oraz potencjalnych sojuszników Hutich, ich arsenał wojskowy oraz ich motywy. Ten temat jest bardziej aktualny niż kiedykolwiek z kilku powodów. Po pierwsze, bezpieczeństwo podmorskiej infrastruktury telekomunikacyjnej ma kluczowe znaczenie dla zapewnienia nieprzerwanego globalnego ruchu internetowego i wymiany danych. Po drugie, aktywna eskalacja konfliktu izraelsko-arabskiego i ataki Hutich na żeglugę na Morzu Czerwonym stwarzają poważne ryzyko i możliwe incydenty, które mogą prowadzić nie tylko do znacznych strat ekonomicznych, ale także do niestabilności geopolitycznej.

W celu przeprowadzenia szczegółowej analizy sprawdzono badania naukowe i artykuły dotyczące wojny domowej w Jemenie, zaangażowania i wsparcia Iranu oraz zapewnienia niezbędnych zasobów wojskowych do ataków na lądzie i morzu, a także fizycznej struktury kabli podmorskich. W artykule szczegółowo przeanalizowano incydent oraz metody i środki, które mogły zostać użyte do przeprowadzenia takiej operacji. Oceniono ekonomiczne i polityczne konsekwencje powtarzających się i poważniejszych uszkodzeń kabli podmorskich. Problem opisany w artykule jest ważny, aby zapobiec wysoce prawdopodobnemu sabotażowi sieci kabli światłowodowych podmorskich i lepiej zrozumieć konsekwencje.

Słowa kluczowe: Huti, kable podmorskie, Jemen, Iran, okręty podwodne.