The Subsea Data Cable Security Map – Fusing Public Information for Enhanced Critical Maritime Infrastructure Security

Jonas Franken
Science and Technology for Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt, Germany
franken@peasec.tu-darmstadt.de
https://orcid.org/0000-0003-0650-0308

Christian Reuter
Science and Technology for Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt, Germany
reuter@peasec.tu-darmstadt.de
https://orcid.org/0000-0003-1920-038X

***Abstract*—This work presents a mapping tool designed to visualize potential risk factors affecting the lifelines of intercontinental communication – subsea data cables. While various geographic information systems provide public data on the oceans, including browser-based maps showcasing maritime fixed infrastructure, these services vary widely in terms of data granularity and functionality. A comparison of different platforms highlights this diversity, with existing maps of subsea infrastructure serving different purposes. However, the absence of an online map tailored specifically to the security needs of critical subsea infrastructure prompted the development of a new mapping solution. The Subsea Data Cable Security Map aims to integrate and display available data on submarine cables and associated risk factors, with a strong focus on usability, modularity, and ease of maintenance.**

***Index Terms*—submarine data cables, critical maritime infrastructure security, geographic information system**

I. Introduction

The Nordstream sabotages of September 2022 have raised public awareness of the security of critical maritime infrastructures (CMI) to a level previously unthought of for maritime issues in Europe [1], [2]. While the background of the disruptions on the Nordstream pipelines remains unknown and the consequences for the European energy market turned out manageable, policy actors on European and national levels have been quite active to accommodate the growing demand to address the lack of subsea CMI security [3]. These processes are supported by increased public interest and awareness after multiple recent faults of fixed CMI on the seabed, like the Balticconnector incident of October 2023, the Svalbard cable incident of January 2022, and the unresolved cable outages in the Red Sea in February 2024 [4]–[6]. A recurring element for future protection pathways of subsea data cables (SDC) is the inclusion and fusion of data on CMI into situational pictures of the maritime space [7], [8]. However, the European Commission acknowledged that *"[c]oncrete elements currently lacking include an accurate mapping of existing cable infrastructures informing a consolidated EU-wide assessment of risks [. . .]"* [9] in a recent White Paper.

Following up the White Paper, the European Commission encouraged member states to conduct *"[...] national risk assessments on the cybersecurity and the physical security of submarine cables infrastructures"* in its Recommendation on Secure and Resilient Submarine Cable Infrastructures of February 2024, adding that *"[t]he national assessments would be more relevant if they include a mapping of the existing and planned infrastructures and if they take into account both technical and non-technical security risk criteria"* [10, p. 10]. This work intends to support EU members in meeting this ambitious objective with regard to SDC.

While outages of the energy sector's CMI are frequently used to justify an uptake of protective measures for SDC, it is important to acknowledge the distinct characteristics that set maritime fossil and electricity infrastructures apart from CMI of the telecommunications sector. First, transmitting over 99 percent of intercontinental data traffic, SDC generally have a more global reach, often spanning the high seas and connecting continents over greater distances than pipelines or energy cables. Second, unlike oil and gas pipelines, the transported goods within data cables – data packets turned light and electric signals – can be quickly rerouted over alternative paths due to their physical properties. On the downside, connectivity cannot be provided through storage like oil or gas. Both aspects support a global rather than a regional perspective of the security of SDC. Third, SDC are less robust than energy cables or pipelines, resulting in more frequent faults, primarily caused by fishing activities or anchoring [11], see Figure 1.

To reduce the frequency of such incidents, especially in shallow and coastal waters, the locations of these cables are

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and supported through the FiF/IANUS-funding of the Technical University of Darmstadt in the project NetzGeschichte. The authors thank the programmer team Ivo Bracharz, Julian Löffler, Manuel Scheurich, Patryk Serafin, Julian Trembilski, Marcel Wagener, and Veit Weidinger for implementing the SDCS Map and conducting the user studies.

generally publicly disclosed. Still, fishing, anchorage, and other human activities around cables, such as sand dredging and seabed mining, account for almost three-thirds of the roughly 150 SDC faults on a yearly average. The remaining 26 percent are split between natural events like seismic activity leading to undersea landslides or tsunamis, technical component failures, and a small proportion of unidentified fault origins. Attributed intended damage to SDC is very rare, with a few cases of cable theft for private gain off Vietnam in 2007 and sabotage attempts in Egyptian waters in 2013 [12]. The last instance of large-scale coordinated sabotages of subsea communication cables even dates back to World War II [13]. However, in times of increasing hybrid threats – for this work defined as efforts by state or non-state actors to exploit vulnerabilities of a target by using a mix of military, economic, or technological measures while remaining below the threshold of formal warfare – malicious actors may prefer to uphold plausible deniability through the imitation of accidental damages such as fishing or anchor damage. The reactions of NATO and EU to the Balticconnector and Svalbard Cable incidents display the current sensitivity to potential hybrid activity against European critical seabed infrastructures [4], [5], [14].

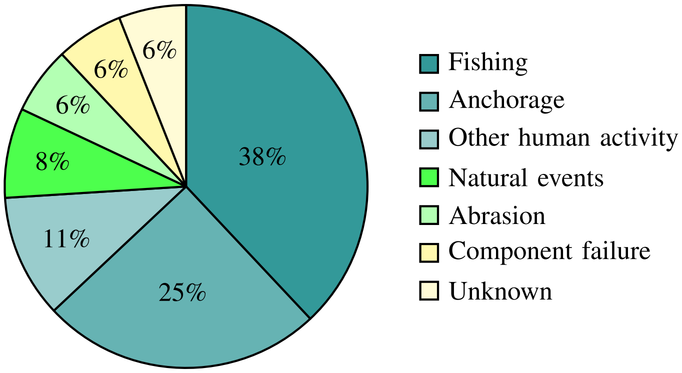

Fig. 1. Subsea cable fault causes, clustered in human activity (blue), environmental causes (green), and other types of origin (yellow). Chart reproduced after [11].

In the following, this work will introduce the authors' approach to mapping SDC together with aspects impacting the availability of their services. In section II, the publicly available data will be presented to showcase the multitude of sources for SDC locations and identify a research gap. Section III presents the artifact called Subsea Data Cable Security Map (SDCS Map), its development process, and evaluation. Section IV discusses various aspects, including the ethical considerations of SDC mapping and an outlook for further enhancements of the SDCS Map, finalized by a conlusion in Section V.

II. Related Works

For the maritime space, the usual visual representations for fused data are maps within geographic information systems (GIS). Similar to the broad choice of maps for sea surface situational picture generation, a plethora of maps entailing subsea infrastructure information is available [15]. Most of these maps are publicly accessible, but there are commercial subscription services as well, see Table I. The largest group of the analyzed maps have been created to serve a commercial purpose, like advertising commercial datasets (M1, M3) or map layers (M12), as a marketplace platform (M10), to support operational SDC project planning (M4) or to foster maritime planning more broadly (M13). Other maps serve non-commercial purposes like shipping safety (M12) and fishery safety (M9) or both (M5). As international organizations with economic development missions, the International Telecommunication Union and the World Bank provide broadband infrastructure mappings that include maritime and terrestrial communication infrastructures (M7, M8). Regarding the data quality and accuracy, large differences can be identified. On the one hand, industry-supplied data of exact locations for safety or installation purposes can be regarded as the best available data quality for SDC locations (M4, M5, M6, M12, M13). Undersea currents or external human activity below the threshold of triggering cable faults may shift SDC locations minimally over time, but these effects are negligible. On the other hand, some maps use a coarser data resolution, either because of aesthetic factors (M1, M2), to promote a more detailed subscription service (M3), or for reasons unknown to the authors (M7). Also, some maps are discontinued (M10, M11) or use outdated SDC layers of other maps (M8), which the authors did not consider for supplying data to the artifact.

While the motivations, roles, available layers, and functions of these map services vary widely, the authors found no approach that includes comprehensive data on factors shaping the availability of SDC services, especially with regard to security issues. The absence of security-focused CMI maps could be due to the lack of attention that maritime infrastructures suffered from in recent decades [2], [16]. Other explanations may be the perceived confidentiality or sensitivity levels of CMI-related data for national and international security actors and business integrity concerns from SDC companies [8].[1] To take on this gap and following the EU Commissions' request for SDC mapping approaches, the following question leads this work: **How can the available data on subsea data cables be fused into a usable visual tool portraying security-related aspects?**

III. Method and Artifact Description

For the development of the Subsea Data Cable Security Map the authors decided on a systematic four-step process. First, the landscape of available maps and data was mapped, see Table I. This entailed conducting a comprehensive review of previous SDC mapping approaches, including their maintainers, status and update frequency, data use licenses, roles and motivations, and data granularity. This step was essential to compiling a diverse range of potential data accesses to be fused in the SDCS Map.

[1] For the discussion of SDC data disclosure ethics, please refer to section IV

TABLE I
Comparison of a Selection of Common SDC Maps.

No.	Map name	Maintaining entities	Role	Status	License	Granularity
M1	*Submarine Cable Map*	Telegeography	Commercial	Active, well-maintained	CC BY-SA 4.0	low
M2	*Submarine Cables of the World*	SubTel Forum (STF)	Industry forum	Active, quarterly updates	Written consent	very low
M3	*World Submarine Cables*	OceaniQ, Global Marine	Commercial	Active, quarterly updates	Restrictive use	medium
M4	*GeoCable® Data & Software*	OceaniQ, Global Marine	Commercial	Active, quarterly updates	Subscription service	very high
M5	*DKCPC Cable Awareness Map*	DKCPC	Safety (DK waters)	Active	Free of charge	very high
M6	*Open Infrastructure Map*	Russ Garrett	Open Data	Active	ODbL v1.0	high
M7	*The World Bank Maps*	World Bank	Econ. development	Active	CC-BY 4.0 & others	low (M1)
M8	*Connectivity Infrastructure Map*	ITU	Econ. development	SDC data from 2020	None mentioned	low (M1)
M9	*KIS-ORCA Map*	ESCA; Kingfisher	Safety (North Sea)	Active	Free of charge	very high
M10	*infrapedia*	Infrapedia	Commercial	Inactive since 2022	MIT License	high
M11	*Greg's Cable Map*	Greg Mahlknecht	Open Data	Inactive since 06/2016	GNU GPL v3.0	medium
M12	*Marinetraffic Nautical Charts*	Kpler	Safety, Commercial	Active	Subscription	high
M13	*MARCO Map*	MARCO/NOAA	Spatial Planning (US)	Active	Free and public	high
M14	***Subsea Data Cable Security Map***	**The authors**	**Security**	**Active**	**EUPL-1.2**	**source-dependent**

Second, the map's architecture was conceptualized, delineating its basic framework and content structure. As a general framework, the authors opted for a browser-based GIS using the JavaScript library Leaflet [17], because it offers a simple Application Programming Interface (API) and rich plugin ecosystem for further customization. Vue.Js was used as user interface framework for its efficiency in dynamic and interactive feature handling for maps [18]. The SDCS Map is optimized for desktop usage while leaving the option for future mobile optimization open. Content-wise, the authors aimed for comprehensiveness, encompassing data on all common types of outage origins. For maritime situational awareness purposes, integrating the highest degree of SDC route granularity is preferable, especially regarding the analysis of security threats from single vessels. The authors integrated the most granular dataset for the North Sea region, KIS-ORCA (M9), to check for the feasibility of detailed SDC route integration. However, the figures below show the SDC routes of Telegeography (M1) that are more decorative and globally available.

For the initial version of security-related layers, emphasis was placed on integrating data related to fishing activities, which is the most prevalent cause of cable faults at about 38 percent of all SDC incidents [11], see Figure 1. Figure 2 displays an exemplary map section showing the intensity of fishing activity in the Bay of Biscay over two days. The fishing data stems from Global Fishing Watch, and can be filtered on a temporal scale by the day back until 01/2017. With these datapoints, fishing activity around SDC can be monitored and provide initial results that can support ex-post analyses of cable fault incidents.

Another layer implemented is the bathymetric layer providing detailed information about the depth and contours of the ocean floor, see Figure 3. This information is essential for determining the safest and most efficient routes for laying subsea data cables, avoiding areas with steep slopes, underwater mountains, and other hazardous topographical features that could pose a risk to the integrity of the cables. It helps identify potential hazards such as underwater canyons, cliffs, and other geological features that could damage cables through abrasion and allows for the anticipation and avoidance of these natural hazards like undersea landslides during the installation and operation phases. Also, sea depth is an important factor in evaluating the risk of cable incidents related to commercial activities. For example, bottom trawling is typically not practiced in depths exceeding 1,000 meters, and the anchor chains of commercial ships usually do not extend beyond 400 meters. As a result, the deep seabed has historically been a safer location for subsea cables, often allowing for the omission of protective sheathing in these deeper areas. However, the increasing interest in deep-sea mining and fisheries exploitation in international waters could alter this situation. Conversely, subsea cable sections in coastal regions, marginal seas, and along maritime chokepoints face an increased risk of damage due to the competing demands on the ocean and seabed.

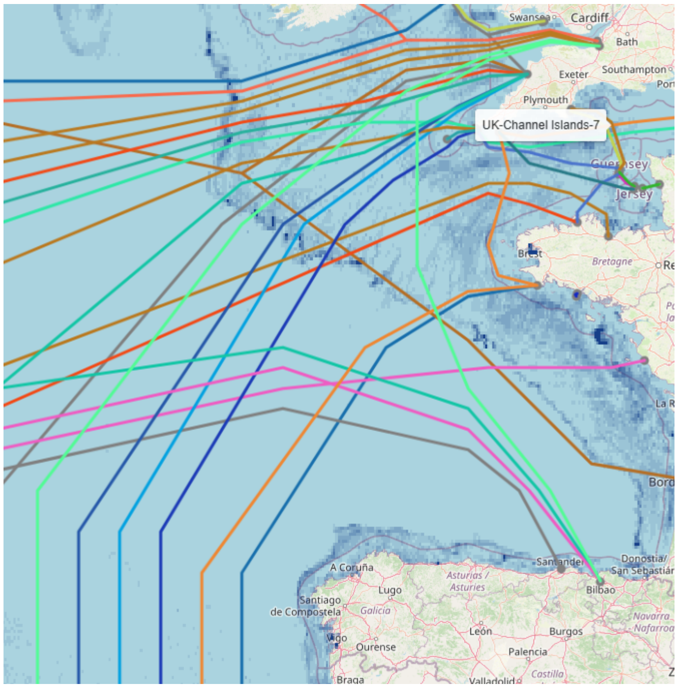

Fig. 2. SDCS Map detail: Fishing activity for 06 March to 07 March 2024 displayed with SDC layers from Telegeography [19].

Relatedly, the third functional layer depicts seismic activity, which is a frequent origin of simultaneous outages of multiple subsea cables. The consequences of underwater landslides

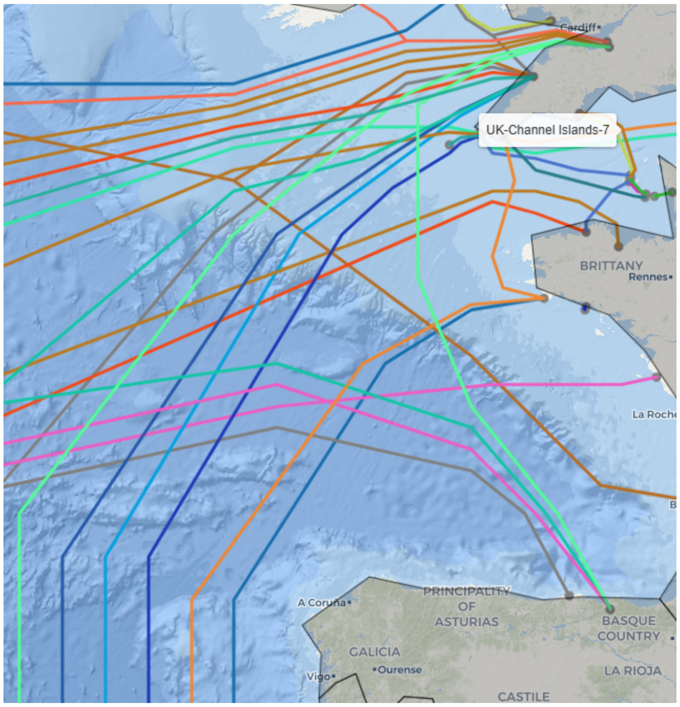

Fig. 3. SDCS Map detail: Bathymetric data of the seafloor displayed with SDC layers from Telegeography [19].

following earthquakes can seen in the Trou Sans Fond incident undersea canyon off Abidjan, which led to outages and slowed internet connections in various countries in Western and Southern Africa in 03/2024 [20]. For the seismic activity layer, see Figure 4, comprehensive and global earthquake data from the United States Geological Survey was used [21]. All of these layers utilize publicly available data continuously updated through the respective APIs of the data sources. Historical records are available for seismic and fishing data. However, the authors determined that the bathymetric structure of the seabed does not change significantly enough to warrant the inclusion of historical seabed data. In subsequent iterations, the authors intend to incorporate additional fault categories; see the discussion in section IV below.

The third step was the iterative implementation of the software design. In the backend, this encompassed the development of a modular architecture, facilitating expandability by containerising databases, tools, and functions. Furthermore, a central database was crafted from various application programming interfaces (API) within the open-source Hasura engine [22], fusing available SDC route data with datasets previously maintained by the authors entailing original, hand-coded variables (e.g., origin of owners, types of ownership, consortia size, and involvement of content providers). Regarding the frontend, the work started by prototyping mock-ups. Based on these, an interactive map interface was devised, featuring clickable submarine data cables, four initial layers (open street map, bathymetric map, seismic, and fishing activity), and optional shapes (territorial waters, contiguous zones, exclusive economic zones, and energy pipeline networks). The user interface design underwent refinement through two iterative rounds of anonymized user studies on various devices and browsers. The user studies included various tasks on each of these layers and shapes that aimed to examine the clarity of the functionalities, performance of the system, and duration of information retrieval.

As a final step, non-sensitive parts of the code will be published under EUPL-1.2 License by 2025 to foster collaboration and national adoption while enabling the integration of additional layers and tools into the mapping platform.

IV. Discussion

Raising awareness for CMIs since the Nordstream sabotages in 2022 increased demand for their protection from natural, unintended, and intended outages. A vast landscape of maps publicly available and with restricted access was found that could inform CMI protection in the future. These GIS artifacts serve many different purposes and audiences, ranging from commercial marketing of paid services to noncommercial open data collection. Accordingly, GIS tools and their underlying functionalities, layers, tools, and databases vary broadly. However, none of these maps specifically focus on issues of security. With the SDCS Map, a basic framework for a modular mapping tool that can fuse live – in the sense of instant update with every API request, which is triggered through switching layers – information from multiple data sources and visualize the status of the global SDC network has been introduced.

The SDCS Map depicts networks often designated as critical infrastructures [23], necessitating an ethical discussion that balances its risks and advantages as new software artifact [24]. The provision of services by SDC is indispensable for the functioning of modern society, making them crucial assets for states. Consequently, the ethical development and deployment of tools like the SDCS Map are paramount, particularly in the context of critical infrastructure protection research.

One of the primary ethical concerns associated with the SDCS Map is the potential for data misuse. Public and nonpublic map services, including those in existence for over two decades, could theoretically be exploited for malicious purposes. For instance, a deliberate cable sabotage could be disguised as a fishing activity or natural event, complicating the detection and attribution of intentional acts. This possibility highlights the importance of incorporating robust security measures like restrictive access to the tool and cautious publication of functions with a higher potential for misuse. Traditionally, the security through obscurity approach has been employed to protect sensitive systems like SDC by concealing their operational details from public knowledge. However, this approach is increasingly ineffective due to the widespread availability of detailed digital nautical charts. In the past, security through obscurity worked only with regard to lay audiences. Anyone with a baseline knowledge of and access to nautical charts, such as commercial fishers and shipping actors, ocean planners, or leisure ocean users would have had the

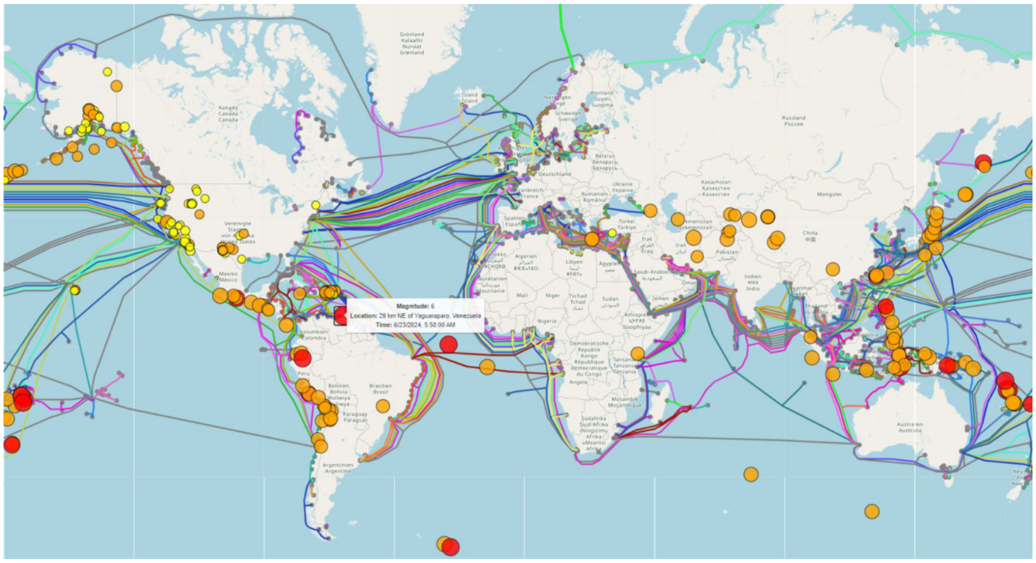
Magnitude: 6
Location: 29 km NE of Yaguaraparo, Venezuela
Time: 6/23/2024, 5:58:00 AM

Fig. 4. SDCS Map: Global view of earthquakes displayed with SDC layers from Telegeography [19].

chance to identify and investigate SDC locations in their map systems. As awareness and accessibility of this information grow, the reliance on obscurity as a single protective layer alone is insufficient. A comprehensive security strategy must now integrate transparency and other protective measures to ensure resilience against potential threats.

The decision by the SDC industry to disclose cable locations freely and establish straightforward licensing regimes for data reuse marked a significant shift toward transparency after the end of the Cold War. This openness was necessary to minimize the large number of unintended damages on the growing network, such as those caused by bottom trawl fishing, which could inadvertently impact cables if SDC locations were unknown. From an operator's financial and legal perspective, the decision to publish route data makes sense, as ocean users without knowledge of the position of cable routes cannot be held liable for negligent behavior. Additionally, the long-term nature of SDC, with a planned lifetime spanning 20-25 years, means that any SDC route data regime or practice shift towards secrecy would take more than a decade to have a meaningful security impact. Moreover, rising repair costs of unintended faults would be the consequence of non-disclosure, as ocean users would not be able to know when to lift their gear. Therefore, transparency of SDC locations remains the better option for maintaining the safety, operational efficiency, and financial viability of SDC in the authors' views.

In the European Union context, the redundancy levels within the SDC network provide resilience against large-scale outages caused by non-state actors. However, state actors capable of coordinated sabotage present a more formidable threat. With frequently observed activities of Russian spy ships near European SDC, state-actor sabotage should not be principally ruled out. Despite this, the secrecy maintained around routing agreements and backup plans by telecommunication companies adds an additional layer of security, complicating the execution of targeted sabotages. Moreover, experimental approaches of the possibilities of public data fusion like the SDCS Map are valuable in supporting political decision-making processes and public scrutiny of protection strategies, ensuring that public spending is allocated effectively and transparently. This open discussion and evaluation of different protection approaches are essential for safeguarding public interests and enhancing the overall security of critical maritime infrastructures.

In the process of setting up the framework, multiple ideas for future enhancement of the SDCS Map emerged: First, implementing interactive tools such as markers, flags, and route manipulation features enhances user engagement and facilitates dynamic analyses of SDC networks. This would allow users to interact more intensely with the map, e.g., to identify key points of interest, flag potential vulnerabilities, and manipulate routes for scenario planning and risk assessment. Second, there is great potential in expanding the inclusion of Automatic Identification System (AIS)-based data beyond fisheries (M5), incorporating both real-time and historical shipping data to provide a comprehensive view of maritime activity. For example, anchoring as the second-most frequent cause of origin for cable damages (see Fig. 1) could be addressed by adding an anchor zones layer and the AIS-based navigational status. At the same time, the authors are aware of the potential for flawed, spoofed, or suppressed AIS information of all types of vessels [25], [26], which necessitates exploring alternative position data sources as well. Addressing this limitation, the map could offer deeper insights into the operational patterns and potential risks associated with SDC infrastructure by integrating individual vessel traffic from AIS and other data sources.

Third, integrating databases and live feeds related to natural disasters, including weather conditions and seismic events, as well as the integration of repair ship tracks, enables proactive risk management and response planning. This feature would equip stakeholders with the necessary primary and secondary information to anticipate and mitigate the impact of outages in SDC networks, ensuring continuity of communication services. Fourth, leveraging Large Language Model-supported web and news scraping for database maintenance ensures the accuracy and timeliness of information updates. For this, the authors envision a text retrieval and analysis tool that could automatically retrieve and suggest relevant data updates from diverse online sources, with the aim of maintaining a current database of SDC infrastructure and associated risks based on the available public data.

V. Conclusion

The issue of the security of critical maritime infrastructure gained momentum after the Nordstream sabotages and recent suspicions of hybrid activities around other incidents such as the Balticconnector or Svalbard cases. Either through public resources requiring taxpayers' money (e.g., increased naval surveillance) or intensified CMI operator requirements (e.g., stricter permitting, obligatory installation or retrofitting of sensor technology), which costs are typically passed on to the end users of the services – reaching an enhanced level of CMI protection will be costly. Therefore, the data that is already publicly available should be leveraged to assess the risks or support the post-analysis of incidents as a low-cost contribution. An overview of publicly available databases (see Table I) revealed there is no approach for a public mapping of security-related factors around the lifelines of the global internet – submarine data cables. It also exposed the general availability of SDC route data, which is disclosed for safety rather than security purposes. Through a user-study-supported, iterative software design approach, the authors created the Subsea Data Cable Security Map that connects cable route datasets of varying granularity with three initial layers of threats to SDC infrastructures: fishing activity, bathymetry, and seismic activity.

The authors are currently working on many of the functionalities suggested in Section IV and invite researchers to reuse public parts of the code to expand the SDCS Map further. The basic SDCS Map will be available at https://SDCS.dev.peasec.de/ under EUPL-1.2 License by 2025. Please contact the first author for a user account and access to the public parts of the code via franken@peasec.tu-darmstadt.de.

References

[1] T. A. Gülcan and K. E. Erginer, ”National and international maritime situational awareness model examples and the effects of North Stream Pipelines sabotage,” *International Journal of Critical Infrastructure Protection*, vol. 42, p. 100624, 2023, doi: 10.1016/j.ijcip.2023.100624.

[2] C. Bueger and T. Liebetrau, “Protecting hidden infrastructure: The security politics of the global submarine data cable network,” *Contemporary Security Policy*, vol. 42, no. 3, pp. 391–413, 2021, doi: 10.1080/13523260.2021.1907129.

[3] M. Freyrie, ”Germany,” in *The Underwater Environment and Europe's Defence and Security*, E. Calcagno and A. Marrone, Eds., Documenti IAI, no. 23, Rome: Instituto Affari Internazionali, 2023. [Online]. Available: https://www.iai.it/sites/default/files/iai2313.pdf

[4] H. Ringbom and A. Lott, ”Sabotage of critical offshore infrastructure: A case study of the Balticconnector incident,” in Maritime Security Law in Hybrid Warfare, Brill Nijhoff, 2024, pp. 155-194.

[5] H. Gulldahl and I. Eriksen, ”This is what the damaged Svalbard cable looked like when it came up from the depths”, *NRK*, Oslo, 26 May 2024. Accessed: Oct. 19, 2024. [Online]. Available: https://www.nrk.no/tromsogfinnmark/this-is-what-the-damaged-svalbard-cable-looked-like

[6] S. Bashfield, ”Defending seabed lines of communication,” Australian Journal of Maritime & Ocean Affairs, pp. 1-13, Oct. 2024. doi: 10.1080/18366503.2024.2363607.

[7] C. Bueger, T. Liebetrau, and J. Franken, *Security threats to undersea communications cables and infrastructure – consequences for the EU*, Brussels: European Parliament, 2022. [Online]. Available: https://www.europarl.europa.eu

[8] G. Soldi et al., ”Space-based global maritime surveillance. Part I: satellite technologies,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 9, pp. 8–28, 2021, doi: 10.1109/MAES.2021.3070862.

[9] European Commission, *”White Paper - How to master Europe's digital infrastructure needs?”* Brussels, Feb. 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

[10] European Commission, *”Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures”*, Brussels, Feb. 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures

[11] A. Mauldin, ”Cable breakage: When and how cables go down,” TeleGeography Blog. Accessed: Oct. 19, 2024. [Online]. Available: https://blog.telegeography.com/what-happens-when-submarine-cables-break

[12] M. Sechrist, “Impact of historic outages,” in *Proceedings of the Reliability of Global Undersea Cable Communications Infrastructure*, Dubai, Oct. 2009. [Online]. Available: https://www.ieee-rogucci.org/report/HTML/files/assets/downloads/

[13] D. R. Headrick, “Strategic and military aspects of submarine telegraph cables, 1851–1945,” in *Communications Under the Seas: The Evolving Cable Network and Its Implications*, B. Finn and D. Yang, Eds., The MIT Press, 2009, p. 0. doi: 10.7551/mitpress/7869.003.0013.

[14] E. M. McNamara, ”Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure” in, *NATO Review*, Accessed: Oct. 10, 2024. [Online]. Available: https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience

[15] J. Franken, T. Reinhold, L. Reichert, and C. Reuter, ”The digital divide in state vulnerability to submarine communications cable failure,” *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100522, 2022, doi: 10.1016/j.ijcip.2022.100522.

[16] J. Franken, F. Schneider, and C. Reuter, ”The internet's plumbing consists of garden hoses: A critical analysis of the advantages and pitfalls of metaphors use for critical maritime infrastructures,” in *Dreizack 23*, H. Schilling, Ed., Kiel: The Kiel Seapower Series, 2023, pp. 1–8.

[17] V. Agafonkin, ”Leaflet.” Accessed: Oct. 19, 2024. [Online]. Available: https://leafletjs.com/

[18] E. You, ”Vue.js,” Accessed: Oct. 19. 2024 [Online]. Available: https://vuejs.org/

[19] TeleGeography, ”Submarine cable map.” Accessed: Oct. 19, 2024. [Online]. Available: https://www.submarinecablemap.com/

[20] N. Booty and M. K. Garzeawu, ”South Africa, Nigeria, Ghana, Liberia and Ivory Coast hit by major internet outages”, *BBC News*, London and Monrovia, 15 Mar. 2024. Accessed: Oct. 19, 2024. [Online]. Available: https://www.bbc.com/news/world-africa-68569022

[21] United States Geological Survey, ”USGS Magnitude 2.5+ Earthquakes.” Accessed: Oct. 19, 2024. [Online]. Available: https://earthquake.usgs.gov/earthquakes/map/

[22] Hasura Inc., ”Hasura.” Accessed: Oct. 19, 2024. [Online]. Available: https://hasura.io/

[23] C. Kavanagh, J. Franken, and W. He, UNIDIR, forthcoming 2024.

[24] J. Franken and C. Reuter, ”Secure critical infrastructures,” in *Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*, 2nd ed., C. Reuter, Ed. Wiesbaden, Germany: Springer Vieweg, 2024.

[25] E. d'Afflisio, P. Braca, and P. Willett, ”Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 4, pp. 2093–2108, 2021.

[26] C. V. Ribeiro, A. Paes, and D. de Oliveira, ”AIS-based maritime anomaly traffic detection: A review,” *Expert Systems with Applications*, vol. 231, p. 120561, Nov. 2023, doi: 10.1016/j.eswa.2023.120561.