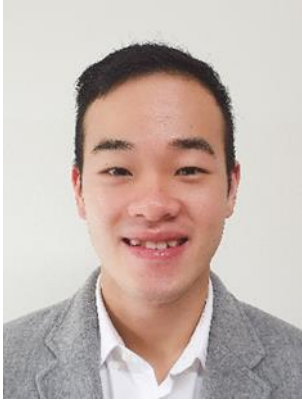


## 부각되지는 않지만 중요한 : 한국의 취약한 해저케이블망 확보

정보의 고속도로로 간주되는 해저 광케이블은 외교와 군사, 금융, 디지털 정보 흐름 촉진에 필수적인 역할을 수행하고 있다. 지금까지 해저 케이블망의 중요성을 조사한 많은 연구가 있었지만, 네트워크 보안과 회복력 강화에 대해서는 그 중요성에 상응하는 노력이 수반되지 않았다. 본고는 한국의 사례 연구를 통해 해저 케이블 영역의 잠재적인 보안 위험을 조명하고자 한다. 한국은 남해안와 일본 대마도 사이의 좁은 초크포인트(chokepoint)에 케이블망이 집중되어 있어 케이블 단절에 특히 취약하다. 이에 점차 불안정해지는 세계 속에서 한국이 해저 케이블망 보안을 강화하는 동시에 국제 정세 안정에 기여하는 중추적인 역할을 할 수 있는 세 가지 접근방법을 제안한다.

\* 본지에 실린 내용은 필자 개인의 의견이며, 태재미래전략연구원이나 그 구성원의 견해나 입장이 아닙니다.

# KIMS Periscope



Taejae Future  
Consensus Institute  
연구원  
Mathew Yeo Jie  
Sheng

## 서론

2022년 1월 발생한 대규모 화산 폭발로 통가와 외부 세계를 연결하는 유일한 해저 광케이블이 끊어지며 통가는 외부 세계와 단절되었다. 통가 내 통신이 두절되어 인터넷 사용과 인도주의적 지원이 어려워졌고, 결국 통가는 유일한 케이블망이 복원될 때까지 몇 주간 혼란에 빠졌다. 통가의 해저 노선은 전세계적으로 현재 운영 중이거나 계획된 약 140만 킬로미터에 달하는 552개의 해저 케이블 중 하나에 불과하다. 더 넓은 맥락에서 살펴보면, 이러한 500여개의 다양한 케이블은 세계 디지털 통신량의 99.4%를 차지하고 있다. 해저 케이블은 매일 약 10조 달러의 금융 송금을 수행하며, 군사 및 외교적 통신 또한 해저 케이블로 전송되고 있다. 위성은 이와 대조적으로 인터넷 접속의 0.37%만을 담당한다. 따라서 세계적으로 막대한 해저케이블의 영향력을 고려한다면, 이처럼 중요한 기반시설의 보안을 유지하고 지속적인 운영을 보장하는 것은 절대적으로 중요하다. 해저 케이블망 보호라는 그 중요성에도 불구하고, "삼중 무적성 (triple invincibility)"에 가려져 절대적인 관심을 받지 못했다. 이에, 본고는 해상교통로 유지의 중요성을 넘어 해저 케이블의 보안적인 측면을 조명하고, 한국이 해저 네트워크 보안강화에 기여할 수 있는 역할을 살펴보고자 한다.

## 해저 케이블의 잠재적인 무기화와 보안 위협

해저 통신 케이블의 보안은 신냉전의 잠재적인 아킬레스건으로 불린다. Tsuruoka는 적이 잠수함, 수중 드론, 잠수부 등의 수중 자산을 통해 국가의 군사, 외교 및 경제 통신을 차단하거나 도청할 수 있다고 지적했다. 실제로 러시아는 우크라이나-러시아 전쟁 초기에 정보전에서 우위를 점하기 위해 우크라이나의 인터넷 기반시설을 가장 먼저 제거하였다. 또한, 2008년 이집트와 이탈리아를 연결하는 해저 케이블 손상으로 인해 이라크에서 미국의 드론 작전이 몇배나 감소했다는 보고가 있었다. 해저 케이블을 통한 도청 및 첩보 활동은 고도로 복잡하고 관련 사례도 적지만, 아예 전례가 없는 것은 아니다. 위키리크스에 따르면, 미국 국가안보국(National Security Agency)과 영국 정부통신본부 (Government Communications Headquarters, GCHQ)가 해저 케이블 도청에 관여한 것으로 나타났다. 해저 케이블에 대한 제도적 규제 부족의 영향은 과거 인식보다

본 발간물은 한국해양전략연구소의 저작물로서 인용 시 표기를 해 주시기 바랍니다.

# KIMS Periscope

훨씬 더 광범위하고 심각하다

해저케이블 통신의 중단이 모두 의도적이거나 악의적인 행위로 인해 발생하는 것은 아니다. 대부분의 통신 단절과 오류는 사고나 자연재해로 인해 일어난다. 님이나 끝났시 조업으로 인한 의도치 않은 케이블 절단이 전체 사례의 66%를 가깝게 차지하는 것으로 나타났다. 그럼에도 불구하고, 계획적인 적대적 통신 단절의 위험은 여전히 존재한다. 해군 전력을 급속도로 증강하고 있는 러시아는 서방과의 전쟁이 본질적으로 '하이브리드' 전이라고 여기고 있으며 이는 미래전에서는 통신 기반시설이 우선적인 목표가 될 것이라는 것을 시사한다. 이와 관련해 러시아는 현재 잠수정 투입을 통해 해저 케이블을 직접적으로 위협할 수 있는 두 개의 해양 자산을 운영하고 있다. 핵추진 Poseidon 수중드론과 Yantar 특수 정보수집함인데 현재는 퇴역한 Losharik '스파이 잠수함'까지도, 수중 케이블을 절단할 수 있는 능력을 충분히 보유한 것으로 알려져 있다. 마찬가지로, 중국은 '수중 만리장성 프로젝트' (Underwater Great Wall Project)의 일환으로 수중 센서, 장비 및 케이블을 조작할 수 있는 자율운항 선박을 투입할 수 있는 능력을 갖추고 있다. 이러한 기술적 발전과 러시아의 은밀한 활동은 해저 케이블에 대한 위협이 상존한다는 것을 보여준다.

## 한국의 취약성

동아시아 지역은 위협으로 가득 차 있다. 이러한 위협을 감지하고 핵심 기반시설 보호의 필요성을 거듭 강조해온 북대서양조약기구 (North Atlantic Treaty Organization, NATO)와 달리, 동아시아 국가들의 집단적인 조치는 거의 찾아볼 수 없다. 이 상황은 한국에게 특히 우려스러운데, 그 이유는 한국의 해저 케이블 9개 중 7개가 폭 50km, 깊이 90m의 좁은 통로를 통과하고 있기 때문이다. 케이블들이 집중되어 있는 이 좁은 초크포인트는 특히 취약하며, 한국에게 우려대상일 수밖에 없다. 이에 더해, O'Malley는 한국이 해저 케이블에 대한 위협을 평가하고 이를 보호할 수 있는 체계적인 접근 방식이 없다고 주장하였다.

따라서 한국은 핵심 기반시설 보호에 더욱 적극적으로 나서야 한다. 첫번째로, 개인 차원에서 해저 케이블의 단절이 한국 사회, 경제와 군 전반에 광범위한 영향을 미칠 수 있다는 점을 고려해 이러한 핵심 기반시설 보호를 국가 안보의 필수 과제로 간주해야 한다. 이를 위해 한국은 자체적인 첨단 모니터링 역량을 개발하는 데 주력해야 한다. 해저 케이블 보호를 위한 선박을 진수한 영국처럼, 한국 역시 케이블의 상태를 모니터링하기 위한 감시선이나 무인선을 도입하거나 건조할 수 있다. 첨단 장비로 민간의 모니터링 및 유지관리 능력을 강화한다면 외부 위협에 대한 해저 케이블 보호 역량을 증진시킬 것이다. 필요한

본 발간물은 한국해양전략연구소의 저작물로서 인용 시 표기를 해 주시기 바랍니다.

# KIMS Periscope

둘째로, 지역 차원에서 한국은 위협 인식을 공유하는 파트너국들을 찾아야 한다. 한국의 11개 해저 케이블 중 10개는 일본이나 대만과 연결되어 있다. 이는 한국이 해저 케이블 보안을 유지하는 데 있어 일본이 필수적인 파트너가 될 수 있음을 시사한다. 마침 일본은 현재 해저 케이블 수를 늘리며 유럽으로의 새로운 경로 개설을 모색하고 있는데, 이로 인해 케이블 훼손이나 단절에 대한 취약성이 증가할 것이다. 이러한 공통된 이해는 일본과 한국이 정보 공유를 통해 자산을 함께 모니터링하고 보호하기 위한 협력의 중요한 출발점이 될 수 있다. 마찬가지로, 한국은 일본처럼 “케이블 연결 및 복원을 위한 쿼드 파트너십 (Quad Partnership for Cable Connectivity and Resilience)”에 참여하여 케이블 기반시설의 유지보수에 대한 쿼드 회원국들의 전문성을 활용할 수 있다. 이러한 다자 협력은 한국의 핵심 기반시설 보호 역량을 배가하는 주요 수단이 될 수 있다.

마지막으로, 해저 케이블과 관련된 국제법 체계에는 상당한 간극이 있다. 유엔해양법협약(UNCLOS)은 해저 케이블에 적용되는 가장 포괄적인 법 체계이다. 그러나 UNCLOS는 첩보행위를 규제하지 않으며, 해저 케이블에 대한 전시 군사 활동과 관련된 명시적인 제약을 제시하지도 않는다. 따라서, 한국은 핵심 기반시설 보호 역량을 강화하는 과정에서 이러한 법적 공백에 대한 국제적 관심을 불러 일으켜 보다 큰 국제적 역할을 수행할 수 있을 것이다. 해저 케이블을 규율하는 법률이 더욱 명확해지면 국가들은 합법적인 행위에 대해 보다 명확한 기준점을 가지게 될 것이며 현재로서는 존재하지 않는 규제력으로 작용할 것이다. 궁극적으로 국가들이 가지고 있는 취약성을 크게 경감시킬 것이다. 이러한 점에서, 한국은 책임 있고 국제법을 준수하는 성숙한 국가로서의 이미지를 제고할 수 있다.

## 결론

해저 케이블 운영 유지의 중요성은 자주 강조되어 왔으며, 여러 연구를 통해 해저 케이블이 금융, 군사, 외교 및 인터넷 정보 흐름촉진에 중요한 역할을 수행하고 있다는 사실이 빠르게 입증되었다. 그러나 이러한 해저 케이블의 중요성에 비해 보안 강화를 위한 노력은 크게 부족했음이 분명하다. 안보 환경이 악화될수록 이러한 직접적이고 만성적인 위협에 대응하는 데 더 많은 노력을 기울여야 한다. 해저 케이블 손상과 단절에 유독 취약한 한국은 해저 케이블망을 보호하기 위해 더 넓은 시각을 가져야 한다. 위에서 언급한 세 가지 접근 방식인 개인, 지역, 그리고 국제적 차원에서 노력을 수행한다면 보이지 않는 위협으로부터 한국의 해저 케이블망을 보호할 수 있는 수단을 확보할 수 있을 것이다.

본 발간물은 한국해양전략연구소의 저작물로서 인용 시 표기를 해 주시기 바랍니다.





## **Unassuming yet Critical: Securing South Korea Vulnerable Subsea Cable Network**

Mathew Yeo Jie Sheng

Associate Research Fellow,

Taejae Future Consensus Institute

*The opinions expressed in this publication are those of the author. They do not purport to reflect the views or positions of Taejae Future Consensus Institute or its members.*

### **Introduction**

In January 2022, a massive volcano eruption severed the only sub-sea fiber-optic cable connecting Tonga to the rest of the world, thereby cutting off Tonga to the outside world. With domestic communication impaired and the internet essentially non-existent, humanitarian efforts were encumbered and the island state was thrown into disarray for weeks until the sole cable was restored. Tonga’s sub-sea line is only one of the 552 active or planned subsea cables in the world, which collectively covers around 1.4 million kilometers worldwide. To put things into perspective, these 500 odd cables are responsible for close to 99.4% of international digital communications traffic - underwater sea cables facilitate around US\$10 trillion in financial transfers daily while military and diplomatic cables are also conducted by the virtues of these cables. In contrast, satellites are only accountable for 0.37% of internet access. Evidently, maintaining security and ensuring the continual operations of these critical infrastructures is paramount given the huge ramifications it can cause globally. Despite its significance, the topic of securing subsea cable networks has not been put with the utmost attention given that it has been clouded with a “triple invincibility”. In this sense, beyond looking at the importance on maintaining these sea lines of communication, this paper aims to shed light on the security aspect of subsea cables and how Korea can play a role in better securing its subsea network.

본 발간물은 한국해양전략연구소의 저작물로서 인용 시 표기를 해 주시기 바랍니다.

## **Potential weaponization and security threats of subsea cables**

The security of underseas communications cables has been termed as a potential Achilles' heel in the next cold war. Tsuruoka noted that an adversary may commit a hostile act via underwater assets such as submarines, underwater drones, and divers that would imperil or even tap into states' military, diplomatic, and economic communications. Indeed, this scenario was elucidated in the earlier parts of Ukraine-Russia war, when Russia first resorted to take out Ukrainian internet infrastructure in order to gain an advantage in the information war. It was also reported that damages to the subsea cable in 2008 between Egypt and Italy resulted in a multifold reduction of US drone operations in Iraq. Although cases of tapping and espionage via subsea cables are still minimal and its workings are greatly sophisticated, it is not unheard of. Wikileaks documents suggest that the National Security Agency of the US and the Government Communications Headquarters (GCHQ) of the United Kingdom have engaged in tapping subsea cables. Evidently, the implications of the lack of institutionalized regulations of subsea cables are far more pervasive and acute than previously realized.

To be sure, not all disruptions are intentional and caused by malicious acts; most faults and disruptions are accidental or acts of nature. It has been reported that unintentional severance of cables via the dropping of boat anchors or trolling accounts for almost 66% of cable interruptions. Nevertheless, the danger of a premeditated and militant disruption is still present, and for good reasons. Russia, which is fast expanding its naval ambitions, regards warfare with the West as inherently 'hybrid', thereby suggesting that future warfare might first target communication infrastructure. Befittingly, Russia currently possesses two known operational sea assets that could deploy submersibles capable of directly threatening the subsea cables. The nuclear-powered Poseidon vessel, the Yantar surface ship, and even the now decommissioned spy submarine Losharik, are believed to be more than capable of severing the underwater cables. Similarly, China is backed by its ability to deploy autonomous vehicles with the ability to manipulate and configure underwater sensors, equipment, and cables as part of its Underwater Great Wall Project. Such developments, coupled with Russian surreptitious behavior which is backed by its capabilities, are testament that the threats of subsea cables are ever-present.

### **South Korea's vulnerability**

Viewed this way, the East Asia region is riddled with threats. Unlike the North Atlantic Treaty Organization (NATO) which has recognized the danger and repeatedly stressed on the

본 발간물은 한국해양전략연구소의 저작물로서 인용 시 표기를 해 주시기 바랍니다.

# KIMS Periscope

need to protect the critical infrastructure, there is little that has been done amongst East Asia states at the collective level. The scenario is particularly worrisome for South Korea, as 7 of South Korea's 9 subsea cables transverse through a narrow passage measuring 50 kilometers wide and 90 meters of depth. This narrow chokepoint where cables are concentrated is exceptionally vulnerable and is an obvious pressure point on South Korea. To make matters worse, O'Malley concluded that South Korea possesses no systematic approach to assessing threats and protecting its vulnerable subsea cables.

In this sense, South Korea must be more proactive in protecting its critical infrastructure. Firstly, at the individual level, given that disruptions to the subsea cables would have far-reaching effects to the Korean society, economy, and military at large, protecting this critical infrastructure should be regarded as a national security imperative. As such, South Korea should look towards the development of its own advanced monitoring capabilities. Similar to the United Kingdom, which has acquired a vessel intended to protect the subsea cables, South Korea can acquire or even develop its own indigenous surveillance ships or unmanned autonomous vehicle to monitor the integrity of its cables. Augmenting the private sector's monitoring and maintenance efforts with better advanced equipment would better ensure that Korea's subsea cables receive their due attention and protection.

Secondly, at the regional level, South Korea should look for partners that share the same concerns. Incidentally, 10 of 11 Korea's cable landings in South Korea also lands in Japan or Taiwan. This conveniently suggests that Japan could be an indispensable partner in maintaining the security of the cables. Opportunely, Japan is currently expanding its number of subsea cables and looking to open new routes to Europe, which would certainly heighten its sense of vulnerability to cable damages or severance. This commonality of interest could be a key starting point for Japan and South Korea to cooperate in collectively monitoring and protecting the assets in the form of intelligence sharing. Similarly, South Korea can also echo Japanese participation of a QUAD initiative titled "Quad Partnership for Cable Connectivity and Resilience" to tap into QUAD members' expertise in maintaining cable infrastructure. This way, such multilateral efforts could be a key multiplier for South Korean efforts to protect its critical infrastructure.

Lastly, significant gaps in the global legal framework pertaining to subsea cable remain. The United Nations Convention on the Laws of the Sea (UNCLOS) is the most comprehensive legal framework that governs subsea cables. Yet, it does not regulate acts of espionage and certainly details no explicit constraints on military actions against subsea cables during wartime. Thus, Korea, in the process of hardening its critical infrastructure, can also play a greater

본 발간물은 한국해양전략연구소의 저작물로서 인용 시 표기를 해 주시기 바랍니다.



international role by garnering international attention towards this legal chasm. Unquestionably, with greater clarity on laws governing subsea cables, states could have a better referent point in what constitutes lawful or unlawful behaviour, thereby providing a restraining force that is currently absent. This would vastly assuage states' sense of vulnerability. In this light, Korea can enhance its image as a responsible and mature law-abiding power.

### **Conclusion**

The significance of maintaining the operations of subsea cables has often been underscored, where studies have been quick to point out its vital role in facilitating financial, military, diplomatic, and web informational flows. However, it is evident that its significance has been disproportionately matched with the efforts undertaken to increase its security. With a worsening security climate, it is imperative that more efforts must be undertaken to address this immediate and chronic threat. In this sense, South Korea, a state that is exceptionally vulnerable to disruptions caused by damages to its subsea cables, must look far and beyond to secure its subsea cable network. This can be done by adopting a three-pronged approach as proposed – undertaking efforts at the individual, regional, and global levels – to generate the powerful critical mass that could better shield Korea from the unseen security threats to its subsea cable networks.

본 발간물은 한국해양전략연구소의 저작물로서 인용 시 표기를 해 주시기 바랍니다.



# KIMS Periscope

## 약력

Mathew는 태재미래전략연구원에서 연구원으로, 미중 관계의 잠재적 협력 요소에 대한 연구를 맡고 있다. 주요 연구분야는 인도-태평양 지역의 안보 문제, 미중 관계, 신흥 국가 및 이들이 세계 질서에 미치는 변혁적인 영향과 국제관계 이론이며 현재 터프츠대학교 플래처 스쿨에서 박사과정을 밟고 있다.

## 국내외 추천 참고자료

- [Lieutenant \(junior grade\) Madison L. Long, “Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks.” U.S Naval Institute. May 2023.](#)
- [Christian BUEGER, Tobias LIEBETRAU, Jonas FRANKEN, “Security threats to undersea communications cables and infrastructure - consequences for the EU”, \*IN-DEPTH ANALYSIS\* - June 2022.](#)
- [Matthew P. Goodman and Matthew Wayland, “Securing Asia’s Subsea Network: U.S. Interests and Strategic Options” CSIS, April 5, 2022.](#)

## 알림

- 본지에 실린 내용은 집필자 개인의 견해이며 본 연구소의 공식입장이 아닙니다.
- KIMS Periscope는 매월 1일, 11일, 21일에 구독자분들께 발송됩니다.
- KIMS Periscope는 안보, 외교 및 해양 분야의 현안 분석 및 전망을 제시합니다.
- KIMS Periscope는 기획 원고로 발행되어 자유기고를 받지 않고 있습니다.

## [웹페이지보기](#)

본 발간물은 한국해양전략연구소의 저작물로서 인용 시 표기를 해 주시기 바랍니다.