KIMS Periscope
For God · For Nation · For Peace

제377호 2025년 3월 11일

커지는 동아시아 해저케이블 안보 위협: 어떻게 대응할 것인가?

국가 간 분쟁이 해저까지 옮겨가며 디지털 시대의 중추적 인프라인 해저 케이블의 취약성이 중대한 안보 위협 요인이 되고 있다. 오늘날 우리는 일상생활의 모든 부분에 걸쳐 디지털 기술과 그 기술에 의해 제공되는 데이터에 의존하여 살아가고 있다. '초연결'(hyper-connectivity)에 의해 지구상 어디에서도 데이터가 실시간으로 공유되는 시대이다.

이러한 상황에서 해저 케이블이 훼손되어 데이터 운반이 원활히 이루어지지 못하는 일이 생기면 우리의 일상생활과 모든 인프라, 사회·경제 활동, 국가 운영에 치명적인 결과가 초래될 수 있다. 국가 안보와 관련하여 중대한 의미를 지니는 것은 전략적, 군사적, 정치적 목적으로 국가 행위자(state actors)나 테러 집단과 같은 비국가 행위자(non-state actors)에 의해 해저 케이블이 훼손(damage)되거나 파괴(sabotage)되어 통신이 방해되거나 차단되는 것이다.

따라서 정부는 해저 케이블 안보의 중대성과 시급성을 인식하고 디지털 시대의 중추 인프라 안보를 위한 적극적인 조치에 나서야 한다. 이를 위해 해저 케이블 안보를 위한 법제 마련에도 나서야 한다.

한서대학교
교수
김 석 균

최근 대만 정부가 자국 북부 해안에서 해저 통신 케이블을 고의로 절단한 혐의를 받고 있는 중국 화물선을 수사하기 위해 한국 해양경찰에 공조 수사를 요청했다는 보도가 있었다. 2023년 2월에도 중국 본토와 대만 섬 사이의 해저 케이블 2개가 중국 어선 및 화물선에 의해 훼손된 사건이 있었다.

국가 간 분쟁이 해저까지 옮겨가며 디지털 시대의 중추적 인프라인 해저 케이블의 취약성이 중대한 안보 위협 요인이 되고 있다. 오늘날 우리는 일상생활의 모든 부분에 걸쳐 디지털 기술과 그 기술에 의해 제공되는 데이터에 의존하여 살아가고 있다. '초연결'(hyper-connectivity)에 의해 지구상 어디에서도 데이터가 실시간으로 공유되는 시대이다.

개인은 인터넷 서비스, 폰 뱅킹, SNS, 이메일, 클라우드 등을 통해 정보를 얻고 소통하며 일상생활과 사회생활을 영위하고 있다. 기업이나 국가는 말할 나위도 없다. 기업 간의 전자상거래, 국제무역, 국제 금융이나 국가 간 통신, 외교, 군사, 교류 활동은 디지털 통신 기술과 그 기술에 의해 제공되는 데이터에 의존하고 있다.

그렇지만 실시간 데이터 공유가 어떤 인프라를 통하여 이루어지고 전송되는지 알고 있는 사람은 많지 않다. 국가 간에 이루어지는 통신의 거의 전부(99%)는 전 세계 바다 밑에 깔린 해저 케이블(submarine cables)에 의존하고 있다.

우주상의 인공위성이 방송 및 GPS 등에 주로 사용되는 데 비해, 해저 케이블은 전 세계 통신 및 인터넷망을 연결하여 데이터의 이동을 원활히 한다. 전 세계 해저에 깔린 총 130만 km에 달하는 464개의 해저 케이블 시스템을 통해 매초 수십 테라바이트(terabytes)의 데이터가 전송되고 있다.

이러한 상황에서 해저 케이블이 훼손되어 데이터 운반이 원활히 이루어지지 못하는 일

이 생기면 우리의 일상생활과 모든 인프라, 사회·경제 활동, 국가 운영에 치명적인 결과가 초래될 수 있다.

사고나 고의적인 해저 케이블 훼손으로 인해 재난적 결과가 종종 일어나고 있다. 2021년 10월 한·중 간 해저 케이블 일부가 끊어져 통신이 먹통이 되었고, 2022년 태평양 섬나라 통가에서는 화산 폭발로 한 달 이상 인터넷 접속이 불가능해 국가 기능이 사실상 마비되었다.

2006년 루손 해협 인근 대만에서 발생한 지진으로 인해 4000미터 깊이 심해에 설치된 7개 케이블 19곳이 손상되어 복구에 49일이 소요되었다. 이 기간 중국, 홍콩, 베트남, 대만, 싱가포르, 일본, 필리핀 등지에서 인터넷 연결 문제가 발생했고, 대만은 사회 전반에 걸쳐 천문학적인 피해를 입었다. 데이터 트래픽이 복구되기 전 항공, 인터넷, 금융, 예약, 이메일 서비스가 중단되었고, 금융시장 및 상업 영역의 기능이 마비되었다.

심해저에 깔린 해저 케이블 훼손은 지진, 화산 폭발 등과 같은 자연재해와 사고나 고의에 의한 인적 활동이 원인이 되고 있다. 해저 케이블 훼손의 80% 이상은 닻을 내리거나 준설 작업, 어로 작업을 하는 과정에서 발생하고 있다.

국가 안보와 관련하여 중대한 의미를 지니는 것은 전략적, 군사적, 정치적 목적으로 국가 행위자(state actors)나 테러 집단과 같은 비국가 행위자(non-state actors)에 의해 해저 케이블이 훼손(damage)되거나 파괴(sabotage)되어 통신이 방해되거나 차단되는 것이다.

두 차례의 세계대전에서 볼 수 있듯이 전시에 해저 케이블 절단은 적국을 혼란시키기 위한 수단으로 활용되고 있다. 평시에도 회색지대 분쟁(grey zone conflicts) 수단으로 이용될 수 있는 위험성이 크다. 테러 집단이나 국가 행위자는 다이버, 유무인 잠수정, 해상 자율주행 물체 등을 이용하여 적대국의 해저 케이블을 훼손할 수 있다. 또는 사이버 공격이나 해킹으로 해저 케이블에 의해 전송되는 데이터를 가로채거나(하이재킹) 운영 시스템을 교란할 수 있다.

AI, 사물 인터넷, 자율주행, 5G 등 클라우드 기반 정보 기술의 고도화와 함께 데이터

의존도는 더욱 커지고 있다. 이에 따라 해저 케이블 안보의 전략적 중요성도 커지고 있지만, 안보 취약성은 개선되지 않고 있다.

심해저라는 물리적 환경, 자연재해나 사고, 의도적 공격 취약성, 케이블망 연결 국가 간 관리 책임 문제, 민간기업 소유·운영에 따른 국가 책임 부과 문제, 국제법상 해저 케이블 보호 규정 미비 등이 위협 요인이 되고 있다.

우리나라는 어느 국가보다 대륙 간 인터넷 사용량이 많은 국가이다. 11개 해저 케이블망은 부산, 거제, 태안에 위치한 3곳의 육양국(landing station)을 통해 외국과 연결된다. 분단으로 실질적인 섬이 되어버린 상황에서 외국과의 국제 통신과 디지털 경제는 전적으로 해저 케이블에 의존하고 있는 실정이다.

디지털 강국임에도 우리나라는 그동안 국제 통신 인프라 구축 및 운용이 미흡하여 일본, 대만 등 타국을 경유한 해저 케이블을 통해 통신을 제공받고 있다. 일본을 거쳐 미국으로 넘어가고, 대만과 중국을 경유해 유럽이나 다른 대륙으로 데이터가 전송되고 있다.

이러한 리스크에 대응하기 위해서는 해저 광케이블망의 이중화(redundancy)가 필수적이다. 미국의 데이터 센터들과 연결되는 한국의 해저 케이블은 단 두 개의 회선으로 연결되어 있다. 이중화는 한 회선이 문제가 생기더라도 데이터를 우회시킬 수 있다.

이와 함께 취약 지점을 파악하여 복원력 향상을 위한 훈련을 하고, 자연재해나 고의적 훼손에 쉽게 손상되지 않도록 보호 장치의 개발이 필요하다. 해군, 해경 함정에도 해저 케이블 위협을 탐지할 수 있는 장비를 탑재하여 운영할 필요가 있다.

정부는 해저 케이블 안보의 중대성과 시급성을 인식하고 디지털 시대의 중추 인프라 안보를 위한 적극적인 조치에 나서야 한다. 이를 위해 해저 케이블 안보를 위한 법제 마련에도 나서야 한다. 디지털 시대에 해저 케이블은 사실상 섬나라인 우리나라를 외부와 연결시켜 주는 바다 속 생명줄과 같다.

약력

김석균 박사는 현재 한서대학교 해양경찰학과 교수로 재직하고 있다. 행정고시를 통해 법제처 사무관으로 공직을 시작하여 해양경찰청장을 역임했다. 동아시아지역의 해양안전 및 안보, 해양분쟁, 해양법집행 등에 대한 다수의 논문과 저서를 발표하며 동아시아 해양문제 전문가로서 국제적 명성을 얻고 있다.

.

국내외 추천 자료

- Mercy A. Kuo. "China's Undersea Cable Sabotage." *The Diplomat.* January 28, 2025.
- David Swan. "What are subsea cables, and what happens when one gets cut?" *The Sydney Morning Herald*. January 04, 2025.
- Sophia Besch and Erik Brown. "Securing Europe's Subsea Data Cables." *Carnegie Endowment for International Peace*. December 16, 2024.

알림

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

웹페이지보기