issue BRIEF

해저케이블망과 데이터 안보

2022-35

고명현 선임연구위원
임정희 선임연구원
아산정책연구원

2022.12.29

1. 서론

지난 9월 26일 서유럽으로 러시아산 가스가 수송되는 발트해 해저에 위치한 노르트스트림(Nord Stream) 가스관이 폭발로 인해 파괴되었다. 아직 폭발 원인이 사고인지 아니면 국가 차원의 공격인지 공식적으로 발표되지는 않았지만 일단 인위적 원인으로 인해 파괴되었고, 그 배후에는 러시아가 있다는 것이 전문가들의 중론이다.[1] 우크라이나 전쟁 전역은 전통적인 육-해-공을 넘어 사이버-우주(스타링크)-전자파(전자전)까지 포괄하는데 이제 해저까지 확대된 것이다.

해저까지 국가간 분쟁이 확장된 배경에는 심해를 가로지르는 해저기간망이 오늘날 세계 경제의 중추적 역할을 하기 때문이다. 해저기간망은 에너지뿐만 아니라 전자상거래-금융거래-통신-IT서비스-디지털 상품 등 데이터를 운반하는 해저케이블도 포함한다. 도리어 서유럽과 러시아를 잇는 해저가스관을 제외하면 해저기간망의 핵심은 데이터 해저케이블이라고 할 수 있다.

데이터 경제의 빠른 성장으로 대륙 간 데이터 트래픽이 기하급수적으로 증가하고 있어 해저케이블의 중요성이 더욱 높아지고 있다. 텔레지오그래피(Telegeography) 통계에 따르면, 2019년과 2020년 사이 전 세계적으로 국제 인터넷 용량이 약 450Tbps에서 600Tbps

이상으로 약 35% 증가했으며, 이 중 유럽이 400Tbps, 아시아가 148Tbps로 두 번째로 많은 용량을 차지한다. 국제 인터넷 광대역의 이동량을 비교했을 때, 유럽의 경우는 75%가 유럽 내 이동으로 그중 25%가 대륙 간 데이터 이동인 점에 반해, 아시아의 경우는 전체 광대역 데이터 이동량의 44%가 대륙 간 이동에 해당한다.[2] 특히 한국이 위치한 동아시아에서는 국가 간 해저 에너지 수송 인프라보다는 데이터 해저케이블망이 크게 활성화되어 있다. 게다가 분단으로 인해 실질적으로 섬이 되어버린 한국의 지리적 특성으로 인해 해저 데이터 케이블망이 국제통신과 디지털 경제에 끼치는 영향은 가히 절대적이라고 할 수 있다. 특히 금융부문에서 해저케이블을 통해 매일 약 10조 달러(한화 약 1경)의 금융 송금이 이루어지며,[3] 클라우드 서비스 및 5G네트워크 확산으로 광대역폭 수요는 2년마다 2배가량 증가할 것으로 예측되고 있다.[4]

해저 데이터 케이블망에는 두 가지 안보적 측면이 중요시된다. 첫째 망 안전, 즉 데이터 송수신 중단 또는 장애를 최소화하는 것이다. 해저 데이터망을 구성하는 광케이블망은 높은 내구성과 신뢰도를 자랑하나 자연재해나 물리적인 공격에 취약하다. 광케이블망에 생기는 물리적 사고나 공격으로 인한 통신장애에서 데이터망을 보호하기 위해서는 광케이블망의 이중화(redundancy)가 필수적이다. 2022년 10월 SK C&C 판교 데이터센터 화재로 발생한 카카오 서비스 장애를 포함한 혼란과 경제적 손실이 보여주듯 핵심 데이터 인프라의 중복구성은 망 안전에 필수적인 요소이다. 해당 사고로 최대 127시간 33분간 장애가 발생했으며, 접수된 피해 건수만 10만 건이 넘는다.[5] 또한 경제적 손실은 약 6000억으로 추정되고 있다.[6] 그러나, 서비스가 마비되어 초래된 개인 및 소규모 기업의 피해, 사회적 영향을 포함한다면 그 이상의 막대한 영향을 초래했다고 볼 수 있을 것이다. 사고 조사 결과를 통해 이중화 미흡, 모니터링 시스템 및 컨트롤타워의 부재, 가용 자원 부족 등으로 원인이 지적되었다.[7] 사회 전 영역에 걸쳐 데이터 및 인터넷망에 의존하여 생활하고 있으면서도 이러한 위험에 대한 인식도, 투자 및 대응책 마련도 사실상 부재했다는 점을 여실히 보여준다. 또한 최근 대만을 둘러싸고 미국과 중국 간의 군사적 충돌 가능성이 높아지면서 대만을 거쳐가는 광케이블에 대한 물리적 공격 가능성이 대두되고 있다. 현재 한국의 해저케이블 회선 상당수가 중국과 공유되고 일본과 대만으로 연결되어 있어 자연재해 및 지정학적 리스크가 크다.

또 다른 안보 리스크 요인은 망보안에 대한 위협으로 외부 세력에 의한, 데이터의 정확성과 일관성을 유지하고 보증하는 '무결성(無缺性, integrity)'의 훼손이다. 여기에는 물리적 및 소프트웨어적 도청이 있다. 19세기부터 부설되기 시작한 해저케이블의 전략적 중요성은 이미 1차 세계대전 당시 영국이 적성국의 통신을 도청하면서 부각되었다. 2차 세계대전 이후 미국과 러시아(구 소련)는 해저케이블 도청을 특수전의 일환으로 격상하였고 심해에서 장기간 잠항할 수 있는 핵잠수함을 기반으로 작전을 진행한다.

물리적인 도청 외에도 데이터 하이재킹(hijacking)을 통한 소프트웨어적 감청도 가능하다. 미국과 이스라엘 연구원들에 의하면 중국은 자국 국영 통신 회사를 통해 한국을 비롯해 미국, 캐나다, 이탈리아, 일본 등의 정부 간, 기업 간 데이터를 가로챘다.[8] 중국이 지리적으로 해저 데이터망의 중심부를 차지하고 세계 인터넷망의 데이터 센터를 확장해 나가고 있기 때문에 중국의 인터넷 데이터 감청 위협은 점점 커질 것이다.

한국의 해저케이블망은 미흡한 이중화로 인해 중국, 일본 등을 경유해 통신을 제공받는다.[9] 대체로 일본을 거쳐 미국으로 넘어가는 구간으로 형성되어 있으며, 현재 한국과 연결된 총 11개의 해저케이블 중에서 중국 또는 일본을 경유하지 않고 미국 및 유럽과 연결되는 회선은 없다. 회선을 공유한다는 것은 그만큼 도청 및 데이터 탈취 등 안보위협에 노출될 가능성이 높다는 것을 의미한다.

우크라이나 전쟁으로 촉발된 해저기간망에 대한 공격과 대만을 둘러싼 미중 간 갈등 사례는 데이터 기간망이 가진 국가안보 내 중추적 위치를 잘 보여준다. 현재 한국의 해저케이블망이 노출되어 있는 리스크로는 (1) 이중화의 부재, (2) 해저케이블 회선을 자연재해 또는 지정학적 위험이 있는 국가들과 공유, (3) 데이터 하이재킹 같은 사이버 공격에 취약 등이라고 할 수 있다. 이를 개선하기 위해 해저케이블 회선 이중화 및 다선화, 통신 단절을 대비하는 훈련, 통신위성에 대한 접근 개선, 긴급상황에서 우주인터넷 활용방안 마련 등을 준비해야만 한다.

여기에는 한국처럼 해저케이블망에 대한 의존도가 높고 지정학적 안보위협에 노출된 대만의 사례를 참고할 필요가 있다. 대만은 자국 해저케이블망에 대한 중국의 위협을 의식해

적극적인 대응전략을 채택하였다. 대만은 15회선에 달하는 기존 해저케이블망 외에도 아예 중국을 통과하지 않는 새로운 해저케이블 회선인 'Apricot'을 2024년 완공을 목표로 건설 중이며 우주인터넷 구축에도 적극적이다. 대만은 700여 개의 기지국을 설치하여 해저케이블망이 완전히 손실될 경우를 대비한다.

우크라이나 전쟁은 유사시 적의 사이버 공격으로 인해 데이터 기간망이 마비될 수 있음을 보여주었다. 오늘날 한국은 세계 10대 경제대국이자 디지털 경제에 크게 의존하고 있음에도 불구하고 소수의 연결점만으로 국제 통신망과 이어져 있어 유사시 한국 경제와 안보를 짓누르는 초크포인트(chokepoint)로 작용할 수 있다. 정부는 이러한 해저케이블망의 취약성을 인지하고, 긴급상황 발생 시 빠른 시일 내에 피해를 복구할 수 있도록 복원력을 강화하고 동맹국들과 정보 공유 및 정책 공조를 확대하여 이중적이고 다양한 회복수단을 마련할 필요가 있다.

2. 한국의 해저케이블망

(1) 해저케이블 현황 및 이용

해저케이블은 광섬유를 이용해 전화, 인터넷, 개인 트래픽 전송까지 담당하는 케이블로, 전 세계 데이터 통신의 99%가 해저케이블을 사용하고 있으며, 위성 통신보다 안정적이고 대용량이라는 장점이 있다. 현재 예정 중인 케이블까지 총 130만km을 커버하는 480여 개의 해저케이블이 연결되어 있으며, 1,306개의 기착지가 운용 중(건설 중 포함)에 있다.[10]

지구 상공에 위치한 인공위성이 방송 및 GPS 등에 주로 사용이 된다면, 해저케이블은 전 세계의 통신 및 인터넷망을 연결하여 데이터의 이동을 원활히 하는 역할을 한다. 해저케이블은 육상케이블과 연결되어 국가들 간에 통신이 가능하도록 한다. 해저케이블의 건설은 주로 여러 국가가 컨소시엄을 구성하여 공동으로 투자하는 형태로 건설되며, 투자액을 통해 회선 사용 지분을 획득하게 된다.[11] 국제 해저광케이블은 주로 통신회사에서 보유하는데 운용 중인 한 기업에서 전담하여 포설하기에는 너무 큰 비용이 소요되므로 국제

통신회사 간 공동지분에 투자하여 참여하거나 IRU(Indefeasible Right of User: 해저 국제회선 영속 사용권) 구매를 통해 사용하고 있다.

2016~2020년까지의 추세를 볼 때, 해저케이블 공급업체들은 주로 태평양(Transpacific), 유럽-중동-아프리카(EMEA), 오스트랄라시아(Australasia) 지역에 집중적으로 투자를 하고 있다. 특히 알카텔(Alcatel Submarine Networks, ASN)은 최근 5년간 새로운 프로젝트들을 발주하며 선두를 달리고 있고, 화웨이마린네트워크(Hwawei Marine Network, HWN)는 특히 EMEA지역 중에서도 아프리카 지역에 집중적으로 공을 들이고 있다. 또한 지난 5년간 공급한 케이블 수치를 기반으로 추산해볼 때 100,000km이상의 케이블을 생산한 미국의 SubCom이 1위를 차지하고 있으며, 93,500km 이상을 생산한 ASN이 2위, 61,500km를 생산한 일본의 NEC가 3위를 차지하고 있다. 중국의 화웨이마린이 4위로 추격해오고 있으며, 이러한 추세는 향후에도 당분간 지속될 것으로 보인다. 중국이 국영기업인 화웨이마린을 중심으로 케이블 사업을 확장하는 것은 미국, 일본을 비롯한 태평양 국가들에게 위협요소가 되고 있다.

특징적인 것은 중국의 3대 통신사(China Telecom, China Unicom, China Mobile)가 투자확대를 통해 케이블 소유권 확장을 해 나가고 있다는 점이다. 또한, 미국의 경우 Google, Facebook과 같은 IT기업들이 투자확대를 통해 단독 소유 및 공동 소유권 확장에 공을 들이고 있다. 과거에는 통신사업자가 해저케이블을 주로 설치하고 운영해왔고, 비용부담으로 인해 광케이블이 통과하는 여러 나라의 주요 통신사업자들이 컨소시엄을 구성하여 구축하는 경우가 대다수였다. 그러나, 최근에는 Google, Facebook, Microsoft, Amazon과 같은 IT기업들이 자체적으로 해저케이블에 투자를 하며 전면에 나서고 있다. 구글의 경우 전 세계 해저 광케이블의 8.5% 이상을 차지하고 있으며, 독자적인 케이블도 4개나 보유하고 있다. 컨텐츠들을 제공하는 IT/플랫폼 기업들의 인터넷 수요가 급증함에 따라, 현존하는 케이블을 바탕으로 광대역을 구입하는 대신, 자체적으로 통신 인프라를 구축하기 위해 해저케이블 부설에 투자하고 있다. [12]

이처럼 주요 빅테크(Big Tech) 기업들이 해저케이블 사업에 투자를 확대하는 데에는 데이터 경제와 클라우드 서비스 수요가 증가하고 있기 때문이다. 4차 산업혁명의 핵심 기술인

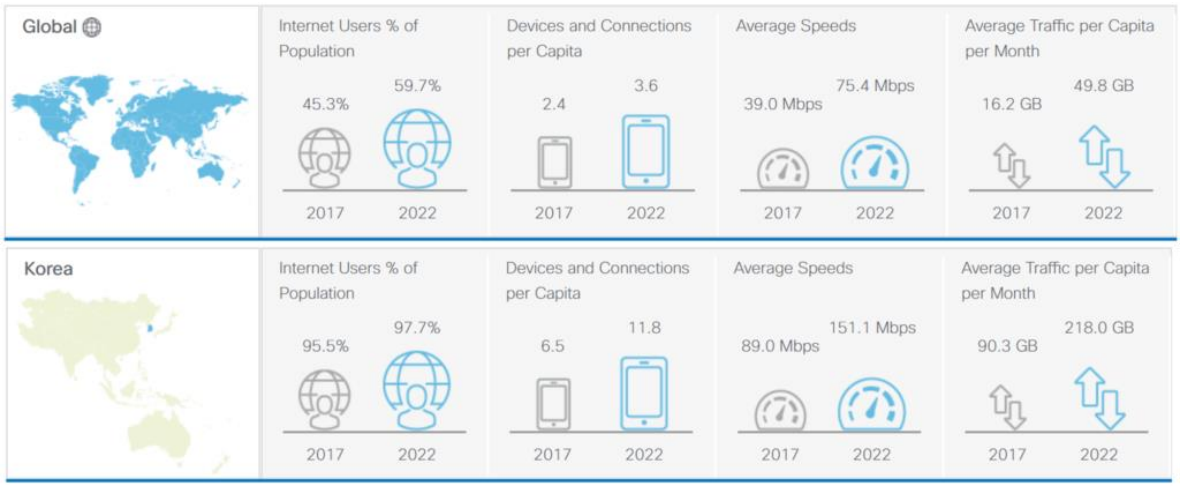
자율주행, 통신(5G), 사물인터넷(IoT), 인공지능(AI), 빅데이터, 핀테크 등 기술 서비스에 핵심적인 인프라 역할을 하는 것이 클라우드이고, 이 클라우드를 뒷받침하는 것이 대규모 데이터 센터와 네트워크, 즉 광케이블망이다. 이처럼 IT기업들은 미래 기술산업의 경쟁력을 확보하기 위해 안정적으로 네트워크망을 구축해야 하고, 이를 위해 독자적인 망 구축을 통해 촘촘한 네트워크망을 구축하려는 것이다. 물리적으로는 이러한 해저케이블을 구축하면서, 각 거점지역에 데이터 센터를 함께 부설하여 데이터 이동의 속도와 안정성을 확보해 나가고 있다.[13]

(2) 한국의 해저케이블 시스템 및 리스크

전 세계 인터넷 사용률(2022년 7월 기준)은 69%에 육박한다. 이 중 아시아 국가들이 차지하는 비중이 54.9%로 절반 이상을 차지한다. 한국은 아시아 국가 중 1.7%를 차지하고 있으며, 국내적으로는 97%에 해당하는 국민이 인터넷에 의존하고 있음을 확인할 수 있다. 절대적으로 많은 인구수를 차지하는 중국, 인도의 경우를 제외하고, 싱가포르(0.2%), 대만(0.8%), 홍콩(0.2%)에 비해 인터넷 사용비율이 높다.[14]

한국의 인터넷 트래픽 양[15]은 2022년 월 인구당 218GB로 2017년에 비해 2.4배 가까이 증가할 것으로 예측되었다. 전 세계 통계에 비해 거의 4배 가까이 많은 수치이다. 실제 무선통신 트래픽 통계를 보면, 2022년 10월 기준 996,799TB을 기록했다. 2015년 10월 기준 177,500TB였던 것을 볼 때, 기하급수적으로 트래픽 양이 증가했음을 확인할 수 있다.[16]

[그림 1] 한국의 인터넷 트래픽



출처: CISCO Korea.

한국에서 해외로 연결되는 해저 케이블은 총 11개이다. 이 케이블은 부산, 거제, 태안에 위치한 국내의 국제 육양국을 통해 해외로 연결된다. 아래의 [표 1]에서 보듯이 거의 대부분의 케이블을 KT가 보유하고 있다. 이외에 2000년에 개통된 제7 국제 해저케이블(SEA-ME-WE3)에 의해 미국을 경유하지 않고 우리나라와 중동 및 유럽 국가들의 인터넷이 연결되었다. 2018년에 완공된 NCP(New Cross Pacific)의 경우 한국과 미국을 직결하는 케이블로, Microsoft 주도하에 KT, Softbank Telecom, China Telecom, China Mobile, China Unicom, 중화통신이 참여하는 컨소시엄 형태로 운영된다. 현재까지 미국과 직결된 케이블의 소유권을 가지는 기업은 KT뿐이다. SK브로드밴드는 KT나 LG와 달리 국내에서 해외로 연결되는 케이블의 지분을 가지지 못하였으나, 2018년 4월 싱가포르-태국-캄보디아-베트남-홍콩-대만-중국-일본-한국 등 아시아 9개국을 연결하는 국제 해저케이블 구축 컨소시엄 SJC2(Southeast-Asia Japan Cable 2)에 참여하며 자체 해외망 확보에 나서고 있다. SJC2는 공사 완공을 앞두고 있다.[17]

[표 1] 한국의 해외 연결 케이블 현황

(단위: km, 년)

케이블명	건설구간	길이	개통연도	사업자	육양지
FEA	한국-일본-홍콩-중동-유럽 등 14개국	29,000	1997	KT	거제
SMW-3	한국-대만-베트남-필리핀-싱가포르-중동-유럽 등 33개국	39,000	1999	KT	거제
APCN2	한국-일본-중국-홍콩-대만-싱가포르-필리핀	19,000	2001	LGU+	부산
KJCN	한국-일본	500	2002	KT	부산
EAC	한국-일본-중국-대만-홍콩-필리핀-싱가포르	19,800	2002	Dacom Crossing (LGU+ 자회사)	태안
C2C	한국-일본-중국 -대만-홍콩-필리핀-싱가포르	17,000	2001	일진C2C	부산
FNAL	한국-일본-중국 -대만-홍콩-필리핀-싱가포르	9,800	2002	서울국제전화	부산
TPE	한국-중국-일본-대만-미국	18,000	2008	KT	거제
APG	한국-중국-일본-대만-홍콩-베트남-태국 -말레이시아-싱가포르	11,000	2016	LGU+	부산
NCP	한국-중국-일본-대만-미국	14,000	2018	KT	부산
SJC2	한국-중국-일본-대만-싱가포르-태국-베트남	10,500	2023 예정	SK Broadband	부산
Bridge one	한국-일본	330	2025 예정	DCT cable	포항

출처: 2020 한국인터넷백서, TeleGeography 참고하여 재구성.

[그림2] 한국의 해외 연결 케이블 지도

출처: Submarine Cable Map.

한국의 국제 통신 인프라 구축 및 운용은 미흡한 실정으로, 일본 등 타국을 경유해 통신을 제공받고 있다. 회선을 공유한다는 것은 그만큼 도청 및 데이터 탈취 등 안보위협에 노출될 가능성이 높다는 것을 의미하며, 회선을 독자적으로 사용하는 것에 비해, 수용가능한 데이터양이 한정되어 있어 트래픽 속도가 상대적으로 느릴 수 있다. 한국의 해저케이블망은 특히 주로 일본을 거쳐 미국으로 넘어가는 구간으로 형성되어 있다. 이러한 이유로 동일본 대지진 때 해저케이블이 손상되면서 대부분의 인터넷이 먹통이 되는 경험을 하였다. 현재 대부분의 구간이 중국, 일본, 대만과 연결되어 있는데, 대만과 일본은 지진 위험이 높고, 중국의 경우 지정학적 리스크가 높으므로, 실제적으로 안정적인 케이블을 구축하고 있다고 안심할 수 없는 상황이다.

(3) 해저케이블의 절단 또는 파괴 시 대응 및 복구조치

국내에서 해외 서버에 접속하기 위해서는 해저케이블을 통해야 한다. 해저케이블이 절단되거나 파괴 및 손상될 시에는 유튜브, 페이스북, 구글과 같은 온라인 서비스뿐만 아니라 해저케이블을 통해 유통되는 데이터를 활용한 모든 인프라, 경제활동, 사회생활,

국가 운영이 마비될 수 있다. 2021년 10월 한중 간의 해저케이블이 일부 끊어져 통신이 먹통이 되었고,[18] 올해 초 태평양 섬나라 통가에서는 화산 폭발로 인해 한 달 이상 인터넷에 접속할 수 없었다.[19]

해저케이블이 손상을 입으면 파손 구간을 수리하고 완전히 복구하기까지 며칠에서 수 주에 가까운 시간이 소요된다. 2006년 루손해협 인근의 대만에서 있었던 지진은 엄청난 사회적·경제적 영향을 초래했다. 4000m 깊이의 7개 케이블의 19곳에 이르는 부분이 손상되었고, 손상되지 않은 케이블도 진흙으로 덮여 있었다. 복구를 위해 11척의 케이블 수리 선박이 동원되었고, 49일의 시간이 걸렸다. 전 지역의 주요 서비스가 마비되었고, 중국, 홍콩, 베트남, 대만, 싱가포르, 일본, 필리핀 등지에서 인터넷 연결 문제가 심각했다. 항공, 금융, 예약, 이메일 이외 모든 서비스가 중단되고 심지어 금융시장 및 상업영역이 모두 막혔다. 대부분의 트래픽이 금방 복구되었음에도 불구하고, 지진이 있은 후 2달이 지나도록 대부분의 트래픽에 영향이 있었다. 동 사례는 해저케이블에 대한 의존도와 중요성을 다시 한번 확인하는 계기가 되었다.

데이터 연결성 및 이러한 인프라에 의존하는 대만 경제에 막대한 경제적 영향을 야기하였다. APEC에서 발간한 보고서에 따르면, 케이블 수리기간을 총 13일로 산정했을 때, 해저케이블 손상으로 인한 복구비용을 경제적 수치로 계산하면, 약 1억 3천 달러에 육박한다.[20] 이 사건은 또한 동 지역에서 해저케이블의 이중화가 되어있지 않았던 폐해를 확인시켜주었다. 해저케이블이 손상되면 데이터가 해당 구간의 다른 케이블로 우회하게 되며, 이 경우 인터넷 및 통신에 품질 문제가 발생할 수 있으므로, 백업이 중요하다. 한국의 경우는 특히 해외 클라우드 서비스 의존도가 높기 때문에 이를 완화시킬 수 있도록 국내 클라우드 산업도 함께 발전시킬 필요가 있다.

3. 해저케이블의 안보적 위협요소

(1) 물리적 요인: 자연재해로 의한 손상

해저 데이터망을 구성하는 광케이블은 높은 내구성과 신뢰도를 자랑하나 자연재해나 물리적인 공격에 취약하다. 2011년 동일본 대지진으로 일본과 연결된 해저케이블이 손상되어 한국도 해외사이트 연결에서 심각한 장애를 겪은 적이 있고, 가장 최근에는 올해 10월 19일 프랑스 남부 해저 광케이블망이 최소 세 군데에서 절단되는 사건으로 유럽뿐만 아니라 미국과 아시아 일부에까지 인터넷 장애가 일어났다.[21] 올해 초 통가에서는 화산폭발로 단일 국제 케이블이 손상되어 한 달 넘게 세계와 거의 단절되었다. 또한 영국의 셰틀랜드 제도와 본토를 연결하는 케이블이 끊어진 후 주민들은 며칠간 모바일 및 광대역 접근에 어려움을 겪었다.

(2) 물리적 공격: 절단(cutting) 및 파괴(sabotage)

망 보안에 대한 대표적인 위협은 외부 세력의 물리적 및 소프트웨어적 감청을 통한 데이터 무결성의 훼손이다. 해저케이블에 대한 위협은 그 역사가 오래되었다. 이미 1차 세계대전 당시 영국은 독일 제국의 외무 장관인 아르투르 치머만(Arthur Zimmermann)이 멕시코 주재 독일 대사에게 멕시코 정부에게 미국에 대항하는 동맹을 제안하라는 지시가 담긴 전보를 감청해 해당 내용을 미국에 전달한 적 있다. 이는 미국이 1차 세계대전에 참전하게 결심하는 원인 중 하나가 된다.

2차 세계대전 이후 미국과 러시아(구 소련)는 해저케이블 감청을 특수전의 일환으로 격상하였고 심해에서 장기간 잠항할 수 있는 핵잠수함을 기반으로 작전을 진행하였다. 현재 미국은 씨울프(Seawolf)급 공격핵잠수함(SSN) 번함인 지미 카터(Jimmy Carter)함에 해저케이블을 도청하거나 파괴할 수 있는 장비를 탑재해 운영한다. 러시아의 경우 팔투스(Paltus)급 또는 로샤리크(Losharik) 소형 핵잠수함 등에 이 같은 임무를 부여한 것으로 알려져 있다. 실제로 러시아는 2014년 우크라이나의 크림반도 침공 시 해저케이블을 절단하여 우크라이나 측의 통신을 차단한 전례가 있다.

해저케이블망의 또 다른 취약지점은 해저케이블이 해저에서 나와 지상 통신망과 연결되는 지점인 국제 육양국(cable landing stations)이다. 한국의 경우 서해 태안, 남해 거제, 동해 부산 3개 국제 육양국 중에서 부산 육양국에만 8개 국제 회선이 접속하여 전체 해저케이블망의 72%를 차지한다. 한국 경제의 IT 및 데이터 산업 의존도에 비추어 볼 때 이중화가 잘 되어 있지 않은 해저케이블망과 국제 육양국에 대한 공격은 매우 치명적일 수 있다. SK C&C 판교 데이터센터 한 곳의 화재로 인해 카카오톡이 완전히 마비되어 복구되는 데까지 5일 이상이 소요되었다는 점을 상기하면 해저케이블망과 육양국의 미흡한 이중화는 망 안전에 대한 중대한 위협이다.

(3) 소프트웨어적 요인: 도청 및 데이터 탈취 사례, 중국의 망 보안 위협

해저케이블망을 둘러싼 또 다른 중대 위협은 소프트웨어적 감청의 일종인 데이터 하이재킹이다. 미 해군대학교와 이스라엘의 텔아비브 대학교 연구자들은 차이나텔레콤(China Telecom)이 국가 간 데이터 트래픽의 원활한 이동을 위해 미국과 캐나다에 위치한 10여 개의 POP(Points of Presence) 서버의 데이터 송수신 경로를 제어하는 BGP(Border Gateway Protocol)[22]를 조작하여 타국 기관과 기업들의 데이터 트래픽을 자국으로 향하도록 한 사실을 밝혀낸 적이 있다.[23]

이러한 중국의 데이터 하이재킹으로 피해를 입은 국가들에는 미국, 캐나다, 이탈리아, 일본 등이 있다. 미국은 2018년 국가 간 송수신되는 데이터가 아닌 미국 국내 데이터가 중국으로 우회된 적이 있으며, 2019년도에는 유럽 이동통신사 데이터가 강제로 우회되기도 하였다. 한국도 예외가 아니어서 2016년 2월부터 8월까지 약 6개월간 차이나텔레콤은 캐나다와 한국 정부 간 통신을 중국으로 가로채 감청한 것으로 알려져 있다.[24]

데이터 하이재킹의 위험성은 중국이 통제하는 해저케이블 회선과 데이터 센터가 늘어날수록 더욱 커진다. 중국은 일대일로 계획의 IT버전이라고 할 수 있는 '디지털 실크로드'를 통해 세계 인터넷에서 자국이 차지하는 비중을 높이려고 한다. 비중이 높다는 것은 그만큼 중국이 통제하는 구역을 통과하는 데이터가 많아진다는 의미이다. 중국은 남미, 아프리카 등 서방국가가 관심을 가지지 않는 빈틈을 파고 들어 전 세계 인터넷의 한 모퉁이를

차지하고 있다. 중국이 일대일로를 따라 부설하고 있는 해저케이블망과 데이터 센터가 완성되면 중국은 인터넷을 마음대로 들여다볼 수 있는 능력을 갖추게 된다.

(4) 지정학적 리스크

[표 1]에서 보듯이 한국의 대부분 해저케이블 회선은 일본을 통해 미국으로 연결되거나 대만 및 중국과 공유된다. 지정학적 충돌가능성 및 자연재해 위험요소가 높은 국가들과 대부분의 회선을 공유하고 있다는 것은 유사시 물리적 훼손이나 도청 위험에 노출될 높다는 것을 의미한다. 당장 GDP 규모가 한국의 절반에 못 미치는 대만이 보유한 해저케이블 회선 수가 15개에 달한다는 점에서 11개에 불과한 한국의 해저케이블 회선 수는 망 안전을 달성하기에 절대적으로 부족한 수량이라고 할 수 있다.

해저케이블과 관련된 지정학적 리스크는 2022년 들어 대만을 둘러싼 미중 간 갈등이 심화되면서 빠르게 커지고 있다고 할 수 있다. 현재 대만을 둘러싼 급변사태 시나리오는 해상봉쇄부터 전면전까지 다양하나, 우크라이나 전쟁은 저강도 분쟁 시에도 기간망, 특히 데이터망에 대한 공격 가능성이 매우 높다는 점을 시사한다. 중국은 주한미군이 주둔하고 있는 한국이 대만사태에 개입하지 않도록 여러 방식으로 견제를 시도할 것이 분명하다. 2016년 차이나 텔레콤의 데이터 하이재킹과 함께 해저케이블망에 대한 공격은 저비용-고효과를 낼 수 있는 대표적 전술이다.

4. 한국의 해저케이블의 보호 및 안정화 방안

국제해저케이블에 의존하고 있는 EU[25], 미국[26], 영국[27], 그 외 한국과 유사한 위치 및 상황에 있는 대만[28], 일본[29] 및 호주, 뉴질랜드 등 각 국가들은 이미 해저케이블에 대한 위협을 인식하고 보호하기 위한 방안들을 마련하고 있다. 동아시아 지역에서도 APEC(호주, 홍콩, 일본, 한국, 말레이시아, 뉴질랜드, 싱가포르, 대만, 태국을 중심으로) 차원에서 2013년까지는 해저케이블 보호를 위한 다양한 방안 및 아태지역 국가 간 협력에 대한 논의가 이루어졌으나 이 이후로는 논의가 진전되지 않고 있다.[30]

앞서 언급된 두 가지 리스크에 대응하기 위해서는 광케이블망의 이중화(redundancy)가 필수적이다. 현재 한국이 가장 데이터를 많이 활용하는 구글 및 페이스북 등 미국의 데이터센터들과 연결되는 광케이블망은 TPE와 NCP 단 두 개의 회선으로 연결되어 있고 전체 해저케이블 회선 수는 11개에 불과해 시스템적 리스크가 크다. 게다가 지정학적으로 신뢰할 만한 인접국이 일본밖에 없는 상황이기 때문에 추가 회선을 중국 또는 러시아와 연결하는 방안은 고려하기 어렵다. 따라서 현존하는 시스템의 이중화, 망 안전과 복원력 향상, 국제 협약을 통한 해저케이블망 보호의 국제법적 근거 확보, 그리고 우주인터넷 구축을 통한 국가 데이터 기간망의 이중화를 강구해야 한다.

(1) 데이터 암호화를 위한 장치

데이터 이중화는 다양한 공격에 취약한 케이블망을 보호하기 위해 필수적인 조치라고 할 수 있다. 네트워크 역량을 다중의 케이블을 통해 보장될 수 있도록 하며, 하나가 마비되거나 차단되었을 때, 다른 케이블을 활용함으로써 차질 없이 네트워크를 사용할 수 있게 된다.[31] 인터넷상 이용되는 모든 데이터 기록은 데이터 센터의 서버에 저장되는데, 이번 카카오 화재 사건과 같이 재난 등으로 소실될 위험에 대비하기 위해서는 두 가지가 필수적이다. 백업으로 알려진 '서버 이중화'이다. 정보의 중요도에 따라 백업과 서버 이중화를 분류해 대비하는 방법도 있다. 카카오 사건의 경우 이원화가 되지 않은 경우에 해당한다. 이원화는 기존 서버가 있는 데이터 센터에서 떨어진 외부에 별도의 백업 데이터 센터를 짓는 방식을 의미한다. 구글의 경우 이미 이러한 이원화 방식으로 데이터 및 서버 이중화 대비를 하고 있었다. 이미 글로벌 빅테크 기업들은 1개 사당 수조원을 들여 이러한 이원화 대비를 하고 있다. 구글 데이터 센터에도 화재가 발생했으나, 구글을 통한 서비스는 마비되지 않았던 이유이다.[32]

또한, 데이터를 전송할 때 그 데이터를 보호하기 위해 암호화를 하며, 이와 함께 물리적 조치나 모니터링을 통해 보호를 강화해야 한다.[33] 해저케이블을 보호하기 위한 조치들은 사실상 해저케이블을 설계하는 단계부터 이루어져야 한다. 케이블 설계자들은 데이터 기밀성(confidentiality), 무결성(integrity) 및 가용성(availability)을 보호하기 위해 필요한

단계들을 거치게 되며 이 과정에서 다층적인 보호가 가능하도록 해야 한다. 미묘한 변화도 탐지하여 네트워크 운영자에게 즉시 통지하도록 하여 타국의 BGP 조작 공격 가능성을 사전에 차단할 수 있도록 보장해야 한다.

(2) 해저케이블망의 이중화

한국과 같은 해저케이블망을 사실상 공유하는 중국이 이미 수차례 데이터를 BGP 조작을 가로챘다는 점에서 대만이 구글과 공동 추진하는 Apricot과 같이 중국을 완전히 배제하는 독자적 케이블망을 구축하는 것이 필요하다. Apricot는 대만, 싱가포르, 필리핀, 일본, 인도네시아, 괌을 연결하는 12,000km 길이의 케이블망으로, 190Tbps 이상의 데이터 용량을 수용한다. 컨소시엄으로 구글, 페이스북 등이 참여하고 있는데, 이 두 회사는 2020년과 2021년에 각각 미 정부로부터 홍콩과 연결하는 기착지를 배제하도록 요구받아 결국 프로젝트를 폐기했던 경험이 있다.[34] 이를 반영해 홍콩을 경유하지 않고, 아시아 6개국을 연결하는 경로로 안정성을 확보할 수 있다는 장점을 가진다.

특히, 최근에 Apricot에 컨소시엄으로 참여하고 있는 PLDT가 필리핀-중국 간의 해양분쟁과 관련된 지정학적 문제를 우회하기 위한 노력으로 필리핀의 Aurora와 Davao섬에 케이블 기착지를 2024년까지 완공할 계획을 공개했는데, 이는 초당 35TB를 초과하는 경우, 데이터 전송 역량을 확대하는 기지국 역할을 할 수 있을 것으로 기대되고 있다.[35] 현재 한국은 아시아-태평양을 가로지르는 3개의 해저케이블 육양국을 구축했으며, 대부분의 회선이 일본과 대만을 경유하고 있다. 이는 주로 남해 지역에 밀집되어 있다. 지정학적 요소에 좌우되지 않을 독자적인 회선 개발을 위해 연구하고 투자할 필요가 있으며, 이와 동시에 안정적인 데이터 전달을 위한 기착지 부설에도 관심을 갖을 필요가 있음을 시사한다.

[그림 3] Apricot 케이블망

출처: Submarine Cable Map

(3) 복원력 및 신뢰성 향상

2006년 대만 강진으로 인해 대만을 통과하는 한국의 국제 해저케이블도 절단되면서 한국의 통신망도 막대한 영향을 받았던 경험이 있다. 보통 해저케이블에 문제 발생 시 우회 경로를 확보하여 데이터 및 인터넷 속도를 복원하도록 하나, 이러한 우회복구는 관련국과 협의하여 이루어져야 하므로, 시간이 지체될 수 있다. 또한, 해저케이블의 손상을 파악하고 이를 수리할 수 있는 선박을 확보하는 데에도 시간이 소요된다. 이러한 이유로 해저케이블 정상 복구에 최소 2-3주가 소요되었다.[36] 일상에서 필수적인 데이터 이용, 무엇보다 은행 및 기업의 전산망이 2주 이상의 공백이 발생할 수 있다는 것은 중대한 안보 위협이라고 할 수 있다. 또한 해저케이블의 손상 시 그 막대한 영향을 고려할 때, 빠른 시일 내에 복원할 수 있도록 복원력을 강화하는 것이 필요하다. 이를 위해서는 동맹국 간의 정보 공유를 확대하고, 케이블이 관리, 유지 및 보호되는 데 있어 어떠한 피해를 방지하기 위해서 사전에 조사할

책임이 있다. 또한 케이블의 경로가 전반적으로 복원력이 보장될 수 있도록 이중적으로, 다양하게 이러한 회복수단을 마련할 필요가 있다.

해저케이블의 절단 및 문제 발생 시 해저케이블을 수리하는 데 있어 가장 중요한 요소는 케이블 수리 선박 및 작업자 등이 얼마나 단시간 내에 작업에 착수할 수 있는지에 달렸다. 현재 해저케이블의 경우 유지보수 협정을 체결하여 관리하고 있다. 각 협정별로 유지보수를 담당하는 케이블 선박이 지정되면 선박소유회사가 해저케이블 소유자를 대신하여 해당 지역에 대기하였다가, 사고발생 시 빠른 시간 내에 출동해 고장지점을 수리 및 복구하게 된다. 현재 KT서브마린이 속한 지역은 요코하마 Zone으로 30개의 통신사업자에 의해 약 20개의 해저케이블이 운용되고 있으나, 이 구간의 대기선박은 2척에 불과하다. 지진 발생 시 관련 해역을 지나는 다수의 해저케이블이 동시에 절단 또는 손상될 수 있음을 고려한다면, 이러한 수리 선박 체계는 분명 한계를 지닌다고 할 수 있다. 따라서 최근에 통신 사업자들이 신규 케이블 시스템을 건설한 후 직접 케이블 선박을 보유하고 있는 공급업자들과 계약을 체결하는 것처럼 지역 협정에 따른 체제 외에 유사시 신속하게 수리에 투입될 수 있는 사설 선박을 확보하는 것도 고려해야 한다.

또한 해저케이블은 네트워크 인프라의 가장 중요한 요소이기 때문에 악의적인 활동으로 보호하기 위해 노력을 다해야 한다. 케이블 소유자 및 운영에 있어 표준 및 지침, 가이드라인을 개발하고, 이러한 표준을 잘 이행할 수 있도록 신뢰성을 확보하는 것이 중요하다. 이를 위해 동맹국과 파트너국이 민간 부문과 협력함으로써 정보 공유를 강화하고 위험 평가를 시행하며, 보안 표준을 마련하고 모니터링 절차 및 수리 역량, 비상시를 위해 비상 계획을 세우는 등의 노력이 필요하다.[37] 해저케이블 보호를 위한 국제법적 보호의무를 촉구하여, 해저케이블을 보호하고, 케이블의 복원력을 보장해야 한다.[38]

(4) 해저케이블 보호의무 강화 및 법적 보호

기존의 국제법적 해저케이블 보호를 위한 협약으로는 1884년 해저전신케이블 보호에 관한 파리 협약(Convention for the Protection of Submarine Telegraph Cables)과 1982년 유엔해양법협약 체제 규정들을 들 수 있다. 1884년 파리협약은 공해상에 위치한

해저케이블만을 대상으로 한다. 제2조에서 해저케이블을 고의나 과실에 의해 파괴하거나 훼손하는 경우 형사책임을 규정하며, 제3조에서는 해저케이블 육양 관련 계약 체결 시 케이블의 트랙은 물론 규모 등과 관해 당사국이 적절한 안전조치를 요구할 수 있는 권한을 규정하고 있다.

1884년 파리협약 제4조에서는 케이블사업자가 케이블을 부설하거나 수리하다가 다른 사업자의 케이블을 파괴하거나, 훼손하는 경우 파괴 또는 훼손비용을 지불해야할 책임을 규정하고 있다. 유엔해양법협약 체제하에서도 해저케이블과 관련한 조항을 제21조, 제51조, 제58조, 제79조, 제87조, 제112조-제115조 및 제297조에서 규정하고 있다.[39] 유엔해양법협약 제113조에서도 공해 아래의 해저케이블을 고의나 과실로 파괴하거나 훼손하는 자국 국적 선박 또는 자국 관할권 내에 존재하는 사람을 처벌하기 위한 입법 의무를 부과하고 있다.

문제는 이 두 협약 모두, 해저케이블의 물리적 훼손을 보호하기 위한 규정만을 두고 있다는 점과 '고의 또는 과실'이 없는 경우, 예컨대 자연재해로 인한 경우나 물리적 충돌 상황으로 인해 파괴 또는 훼손되는 경우에 대해서는 책임을 추궁하는 데 한계가 있다는 점이다. 이와 관련해, 해저케이블을 절단한 경우, 이를 무력공격으로 간주하여 유엔헌장 제51조상의 자위권을 발동할 수 있다는 논의도 진행되고 있다.[40]

특히, 소프트웨어적 측면인 해저케이블을 통한 도청, 데이터 탈취, 하이재킹 등에 대해서는 현존하는 협약이 존재하지 않다는 점에서 현재 해저케이블 관련 국제법적 체제는 큰 한계를 지니고 있다고 할 수 있다. 이와 관련해서 Tallin Manual 2.0[41]상에서 이에 적용가능한 규칙들을 확인할 수 있다. 예컨대 규칙 32에서는 평시 사이버 첩보활동(espionage)[42]을 규제하는 내용을 포함하며, 규칙 4에 따르면 도청(tapping)을 통한 데이터 하이재킹을 주권침해로 볼 수 있다. 이외에도 규칙54에서는 해저케이블 관련 내용을 별도로 규정하고 있다. 그러나 Tallin Manual은 현재 법적 구속력이 있는 문서는 아니다. 따라서 현존하는 해저케이블 관련 협약의 한계를 보완할 수 있는 Tallin Manual을 규범화하고, 각 국가가 국내적으로도 입법 및 실행을 통해 이를 반영할 필요가 있다. 사실상 1884년 파리협약은

체결된 지 너무 오래되어 현실 상황을 규율하는 데 한계가 있으므로, 해저케이블을 통한 다양한 위협요소를 포괄하는 새로운 협약 체결을 위한 노력이 요구된다.

(5) 우주인터넷

대표적인 인공위성 무선인터넷은 SpaceX의 '스타링크', 영국 우주인터넷 기업 '원웹'이 있다. 인공위성 무선인터넷은 인터넷 다운로드 속도가 80~150Mbps 수준으로, 5G 통신망의 다운로드 속도가 690.47Mbps임을 감안하면 속도 측면에서는 기존 광케이블망을 대체하기에는 느리다고 할 수 있다. 그러나 스타링크의 경우 현재도 비즈니스 모델에는 더 비싼 사용료를 받는 대신 500Mbps 속도까지 제공하고 있음을 고려할 때, 향후 위성인터넷의 속도는 더 개선될 수 있을 것으로 보인다.[43]

또한 우주인터넷은 저지연성 측면에서 강점을 가진다. LTE의 지연율이 0.02초인데 비해, 우주인터넷은 0.025초로 유사한 수준이며, 해저케이블이 0.07초임을 고려할 때 낮은 수준이라고 할 수 있다. SpaceX가 목표로 하고 있는 1Gbps까지 달성한다면, 한국의 평균 인터넷 속도 대비 최대 40배 빠른 인터넷을 사용할 수 있게 된다.

비용 측면에서는 초기 설치비용이 약 599달러(약 76만원), 월 사용료가 110달러(약 14만원)임[44]을 고려하면 기존의 광대역인터넷 사용료에 비해 저렴하다고는 볼 수 없지만, 향후 비용 측면에서도 감소할 것으로 밝혔으므로, 현재보다는 저렴한 비용으로 이용이 가능할 것으로 보인다. 해저케이블이 손상되면 그 복구까지 시간이 많이 소요됨을 고려할 때, 대안 인터넷으로는 충분히 기능할 수 있을 것으로 본다. 또한 대안 차원에서 투자한다는 측면을 고려한다면 비용부담이 크다고는 볼 수 없을 것이다.

이미 우크라이나 전쟁에서 일론 머스크(Elon Musk)의 스타링크(Starlink)가 우주인터넷이 지상 데이터망을 대체할 수 있음을 충분히 보여주었다. 특히 스타링크의 강점은 무선 통신임에도 불구하고 망 안정성이 매우 우수하다는 점이다. 일차적으로 통신 암호화가 내재되어 감청이 어려우며 최대 4만여 대 달할 계획인 스타링크 위성들을 공격한다고 해도 높은 이중화로 인해 우주인터넷의 완전한 마비는 거의 불가능하다. 또한 통가의 사례와

같이 해저케이블 설치가 어려운 지역에는 대안위성으로 사용될 수 있으며, 위성인터넷의 경우 낮은 고도에서 많은 수의 위성을 설치하여 운영하므로, 지연시간이나 대기시간을 줄일 수 있다는 장점도 있다. 게다가 파괴될 경우 확산될 위성 파편 때문에 주변의 중국과 러시아 위성들도 피해를 볼 수 있어 스타링크에 대한 공격 가능성은 매우 낮다고 할 수 있다.[45]

대만의 경우 우크라이나 해저케이블망이 완전히 손실될 경우를 대비하여 700여 개의 우주인터넷 통신기지를 구축할 계획이다. 대만이 준비 중인 우주인터넷은 비상망과 상업망으로 구성되어 평시에는 상업망을 통해 인터넷 사각지역을 연결할 계획으로 알려져 있다. [46]

5. 결론: 해저케이블망의 복원력 강화와 이중화

사이버 영역이 확대되고 많은 서비스가 물리 영역에서 사이버 영역으로 이동하면서 국경의 의미가 희미해지고 있지만 아이러니하게도 물리적 기간망의 중요성은 더욱 커지고 있다. 게다가 우크라이나전쟁은 데이터 기간망이 공격과 방어에서 필수적임을 다시 한번 확인해 주었다. 특히 전쟁 초기 러시아가 우크라이나 통신망을 장악하지 못한 데는 미국을 위시한 나토 국가들의 지원에 힘입은 바가 크다. 미국과 일론 머스크가 스타링크로 대표되는 우주인터넷을 우크라이나에 대체재로 제공하지 않았다면 현재 전황은 러시아에게 훨씬 유리했을 것이다.

우크라이나 전쟁은 향후 국가안보에 있어서 데이터 기간망의 이중화가 매우 절실하다는 점을 보여준다. 한국의 경우 해외와 연결을 가능케 하는 해저케이블망이 국가 기간망의 핵심이라고 할 수 있다. 그러나 유사시 국가 해저케이블망을 외부 공격에서 어떻게 보호할 것이며, 파괴되었을 경우 어떤 대안이 있는지 아직 구체적인 정책이 없는 상황이다.

이는 해저케이블망에 대한 의존도가 높고 지정학적 안보위협에 노출된 대만이 적극적으로 대응전략을 수립한 것과 대비된다. 대만은 자국 해저케이블망에 대한 중국의 위협을 의식하여 15회선에 달하는 기존 해저케이블망 외에도 아예 중국을 통과하지 않는 새로운 해저케이블 회선인 'Apricot'을 2024년 완공을 목표로 건설 중이며 우주인터넷 구축에도

적극적이다. 대만은 700여 개의 기지국을 설치하여 해저케이블망이 완전히 손실될 경우를 대비하고 있다.

한국 해저케이블망의 리스크로는 (1) 이중화의 부재, (2) 해저케이블 회선을 자연재해 또는 지정학적 위험이 있는 국가들과 공유, (3) 데이터 하이재킹 같은 사이버 공격에 취약 등이라고 할 수 있다. 이를 개선하기 위해 해저케이블 회선 이중화 및 다선화, 통신 단절을 대비하는 훈련, 통신위성에 대한 접근 개선, 긴급상황에서 우주인터넷 활용방안 마련 등을 준비해야만 한다.

이와 관련해 미국, 일본, 호주는 정보공유를 확대하고 전략적으로 중요한 지역의 해저케이블 사업에서 자금협력 등을 통해 신뢰가능한 통신망 확산을 위해 해저케이블 분야 협력을 강화해 나가고 있다.[47] 동맹국 및 뜻을 같이 하는 국가들과 파트너십을 통해 해저케이블망을 보호하는 국제법적 근거를 강화해 국가행위자에 의한 위협을 억지하고 공격 시 대응할 수 있는 법제 및 국제 공조 체제를 마련하는 것이 필요하다. 또한 해저케이블망뿐만 아니라 국가기간망의 데이터 트래픽의 무결성을 보호하기 위해 미국과 동맹이 추진하는 망 안전 정책에 적극 동참하고, 데이터 무결성이 보장되지 않는 국가 시스템을 필히 우회하며 해당 국가가 제조한 네트워크 하드웨어와 소프트웨어를 국가 기간망에서 배제하는 것이 필요하다.

그 무엇보다도 중요한 것은 해저케이블과 여기에 이동하는 데이터의 무결성이 침해되었을 때 빠른 시일 내에 피해를 복원할 수 있도록 복원력을 강화하는 것이다. 이를 위해서는 뜻이 맞는 국가들과 정보 공유 및 정책 공조를 확대하고, 해저케이블이 관리, 유지 및 보호되는 데 있어 어떠한 피해를 방지하기 위해서 사전에 조사할 책임이 있다. 또한 케이블의 경로가 전반적으로 복원력을 보장할 수 있도록 이중적으로, 다양하게 이러한 회복수단을 마련할 필요가 있다.

지정학적으로 섬과 다를 바 없는 한국은 세계 10대 경제대국임에도 불구하고 겨우 11개의 해저케이블 회선과 단 3개의 육양국으로 세계와 연결되어 있으며, 해저케이블의 현실적 대안인 우주인터넷의 활용도는 매우 미미한 실정이다. 이 작은 수의 연결점들은 유사시

한국 경제와 안보를 옥죄는 초크포인트(chokepoint)로 작용할 수 있다. 한국 국제 데이터망의 구조적 취약성은 최근 해저케이블망에 대한 위협이 현실화되면서 더욱 증폭될 것이다. 국가 데이터망의 이중화-복원력 강화와 동맹과의 공조를 통한 국가 차원의 망 안정성 확보가 시급한 이유이다.

---

[1] The Economist, "Vladimir Putin says the world's energy infrastructure is "at risk"", Oct. 20, 2022, https://www.economist.com/international/2022/10/20/vladimir-putin-says-the-worlds-energy-infrastructure-is-at-risk

[2] TeleGeography, Global Internet Map 2021, https://global-internet-map-2021.telegeography.com/

[3] Government technology, "Undersea Cables: Too Valuable to Leave Vulnerable?", Dec. 12, 2017, https://www.govtech.com/network/undersea-cables-too-valuable-to-leave-vulnerable.html

[4] Submarine telecoms Forum, "Industry Report 2021/2022", Oct. 25, 2021, https://subtelforum.com/submarine-telecoms-industry-report-10th-anniversary-issue-now-available/, Colin Wall, "Invisible and Vital: Undersea Cables and Transatlantic Security", *CSIS*, Jun. 11, 2021, p. 4. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

[5] 과학기술정보통신부, 보도자료,「디지털서비스 장애 조사결과 발표, 시정요구- SK C&C, 카카오, 네이버에 이행결과 및 향후 계획 1개월내 제출토록 -」, 2022.12.6, https://www.korea.kr/news/policyNewsView.do?newsId=156540855

[6] 증권업계에서는 화재사고 이후 하루 매출 200억 원 내외의 손실이 발생했을 것으로 추산하였고, 소상공인 현금보상금 및 1차 서비스 유료 보상금 400억, 일반 이용자 대상으로 제공될 보상금액 및 기타 보상금을 포함하면 5500억을 넘어선다. 서울경제, "카카오 "유료서비스 보상액은 400억 정도 예상"" (2022. 10. 24), https://m.sedaily.com/NewsView/26CH54V9XA#cb, 경향신문, "카카오, 2일 비대위 해체…SK C&C 구상권 논의 본격화하나" (2023. 1. 1), https://m.khan.co.kr/it/it-general/article/202301011721001#c2b.

[7] 카카오 개발자 컨퍼런스, "1015 장애 원인 분석", https://if.kakao.com/2022/session/111.

[8] Demchak, Chris C. and Shavitt, Yuval, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs*: Vol. 3: Issue. 1, Article 7, 2018, pp.1-10.

[9] Industry News, "테크공룡들, 땅에서는 데이터센터 수면 아래선 해저케이블 힘겨루기" (2021. 4. 12), https://www.industrynews.co.kr/news/articleView.html?idxno=41967

[10] Submarine Cable Map 2022, https://submarine-cable-map-2022.telegeography.com/.

[11] 홍성남,「해저케이블 건설공사 소개」,『해안과 해양』3권 1호, p. 51.

[12] Submarine telecoms Forum, "Submarine Telecoms Forum", Issue 127, Nov. 2022, p. 11.

[13] "How Undersea Cable Drive Onshore Site Decisions", Site Selection Magazine, Mar. 2020, https://siteselection.com/issues/2020/mar/data-centers-how-undersea-cables-drive-onshore-site-decisions.cfm

[14] Miniwatts Marketing Group, Internet World Stats, Internet 2022 Usage in Asia, https://www.internetworldstats.com/stats3.htm

[15] 트래픽(traffic)은 통신분야에서 통신망에서 전송되는 데이터의 양을 의미하는 것으로, 모바일 트래픽은 무선통신에서 전파를 이용하여 전송되는 정보량을 의미한다. 장재혁, 박승근,「모바일 트래픽 동향」, ETRI, pp.107-108 참고.

[16] ICT 통계포털, 무선통신 기술방식별 트래픽 현황, itstat.go.kr/itstat/kor/tblInfo/TblInfoList.html?vw_cd=MT_ATITLE#tbl_list

[17] Insight Korea, "SK브로드밴드, 아시아 9개국 연결 국제 해저 케이블 완공 '초읽기'" (2021. 6. 1), http://www.insightkorea.co.kr/news/articleView.html?idxno=89005

[18] YTN, "한-중 해저 케이블 일부 끊어져… 일부 통신 '먹통' (2021. 10. 24) , https://www.ytn.co.kr/_ln/0104_202110241404417156

[19] 머니투데이, "'초연결 세계' 무너뜨린 해저화산…한국 인터넷은 안전할까" (2022. 1. 22), https://news.mt.co.kr/mtview.php?no=2022012113512135491

[20] Asia-Pacific Economic Cooperation, "Economic Impact of Submarine Cable Disruptions", APEC Policy Support Unit, December 2012, pp.36-37 참고.

[21] AP News, "French Polich probe multiple cuts of major internet cables", Oct. 22, 2022, https://apnews.com/article/technology-europe-france-marseille-business-49d27ccc0195f1c48b33a5634232031f

[22] BGP란, 데이터 라우팅을 가능하게 함으로써, 인터넷을 작동하게 하는 프로토콜을 의미한다. 예컨대, A국에 있는 사용자가 B국의 원본 서버가 있는 웹사이트를 로드하면 이러한 통신이 빠르고 효율적으로 이루어지도록 하는 프로토콜을 말한다. BGP 하이재킹은 공격자가 악의적으로 인터넷 트래픽을 재라우팅하는 것으로, 잘못된 방향으로 향하도록 하거나, 정보를 모니터링하거나 가로채는 등의 결과를 초래한다. Cloudflare 사이트 참고, https://www.cloudflare.com/ko-kr/learning/security/glossary/bgp-hijacking/

[23] 앞의 주 3 참고.

[24] 앞의 주 3, pp. 5-6.

[25] Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers, Oct. 22, 2020, https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en, Euractiv, "NATO seeks ways of protecting undersea cables from Russian attacks", Oct. 23, 2020, https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/, European Parliament, Security threats to undersea communications cables and infrastructure – consequences for the EU", https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557.

[26] CRS, "Undersea Telecommunication Cables:Technology Overview and Issues for Congress", Sep. 13, 2022, https://crsreports.congress.gov/product/pdf/R/R47237, NBR, Backgrounder from the Maritime Awareness Project Submarine Cables, https://www.nbr.org/publication/submarine-cables/, Knowledge at Wharton, "Managing Risks for the World's Undersea Cable Network", Nov. 2, 2015, https://knowledge.wharton.upenn.edu/article/managing-risks-for-the-worlds-undersea-cable-network/

[27] Navy Lookout, "The threat to world's communications backbone – the vulnerability of undersea cables", Mar. 10, 2021, https://www.navylookout.com/the-threat-to-worlds-communications-backbone-the-

vulnerability-of-undersea-cables/, Rishi Sunak MP, "Undersea Cables: Indispensable, insecure", *Policy Exchange*, Dec. 1, 2017, https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/

[28] Ministry of Digital Affairs, Meeting with ICANN Jia Rong Low, https://moda.gov.tw/en/press/background-information/3086, The Japantimes, "Taiwan tensions raise alarms over risks to world's subsea cables", Oct. 31, 2022, https://www.japantimes.co.jp/news/2022/10/31/asia-pacific/taiwan-tensions-subsea-cables/

[29] Datacenter Forum, "Government Japan Disperses Submarine cable bases to reduce security risks, Jan. 13, 2022, https://www.datacenter-forum.com/datacenter-forum/government-japan-disperses-submarine-cable-bases-to-reduce-security-risks, The Japantimes, "Undersea internet cables offer more resilient connection", Nov. 24, 2020, https://www.japantimes.co.jp/opinion/2020/11/24/commentary/world-commentary/undersea-internet-cables-japan/

[30] APEC Committee on Trade and Investment, APEC: Submarine cable resilience critical to connectivity, Feb. 06, 2013, https://www.apec.org/press/news-releases/2013/0206_cable APEC, "Economic Impact of Submarine Cable Disruptions", Feb. 2013, https://www.apec.org/publications/2013/02/economic-impact-of-submarine-cable-disruptions

[31] TeleGeography Blog, "Submarine Cable Redundancy, Explained", https://blog.telegeography.com/what-is-submarine-cable-redundancy

[32] 매일경제, "'쌍둥이 데이터센터'있었다면…초유의 카톡 먹통 막았다" (2022.10.31), https://m.mk.co.kr/news/it/10509448

[33] Jonathan E. Hilman, "Securing the Subsea Network: A Primer for Policymakers", CSIS, Mar. 9, 2021, p.9

[34] The Register, "Google and Facebook abandon Hong Kong landing of new submarine cable, Aug. 31, 2020, https://www.theregister.com/2020/08/31/google_facebook_drop_hong_kong_cable/

[35] Submarine telecoms Forum, "PLDT to Fast Track Construction of Cable Landing Stations, Dec. 5, 2022, https://subtelforum.com/pldt-to-fast-track-cable-landing-stations/

[36] 당시 KT국제전용회선 92회선, 데이콤 국제전용회선 43회선을 포함해 대만을 통과하는 한국의 국제해저케이블 135회선이 절단되었다. 이로 인해 국민은행, 외환은행, 메트라이프 등 금융기관과 외교통상부, 로이터통신, 포스데이타 등 은행 및 기업, 정부기관 27개사의 전산망이 통신서비스 마비로 차질을 입었다. 중앙일보, "대만지진 국내 피해기업 40여곳" (2006. 12. 27), https://www.joongang.co.kr/article/2549137, 조선일보, "대만, 지진으로 해저광케이블 손상 '인터넷대란'" (2006. 12. 27), https://www.chosun.com/site/data/html_dir/2006/12/27/2006122700848.html

[37] Christian Bueger, Tobias Liebetrau, Jonas Franken, "Security threats to undersea communications cable and infrastructure-consequences fo the EU", European Parliament 참고.

[38] 앞의 주 4, Colin Wall, ibid, pp.6-9.

[39] 신창훈,「동북아시아 해저케이블의 보호·유지 및 수리문제와 관련한 국제법 및 국내법 동향」, 『서울국제법연구』, 16권 1호, pp.103-139 참고.

[40] 이기범, 해저 케이블의 보호와 국제법, 아산정책연구원, 2020. 12. 14.

[41] Tallin Manual은 NATO 사이버방위협력전문센터(NATO CCDCOE)에서 주도로 사이버 공간에서 발생하는 다양할 활동 및 무력 충돌을 규율하기 위한 국제법적 법률화 작업의 결과물로, 2013년에 1.0, 2017년에 2.0을 발간하고, 2021년 3.0을 위한 작업을 진행중이다.

[42] 규칙32에 따르면, 사이버 첩보활동이란, 전자적으로 전송되거나 저장된 통신, 데이터, 또는 기타 정보를 감시, 감독, 탈취 또는 추출하는 데 사이버 역량을 이용하는 것과 관련되며, 이에 한정되는 것은 아니라고 명시하고 있다.

[43] SatelliteInternet.com, https://www.satelliteinternet.com/

[44] SatelliteInternet.com, https://www.satelliteinternet.com/

[45] The Straits Times, "Taiwan plans for Ukraine-style back-up satellite Internet network amid risk of war", Sep. 22, 2022, https://www.straitstimes.com/asia/east-asia/taiwan-plans-for-ukraine-style-back-up-satellite-internet-network-amid-risk-of-war.

[46] Handelsblatt, "Lessons from the Ukraine War: How Taiwan Is Building a Digital Fortress", Feb. 12, 2022, https://www.handelsblatt.com/politik/international/satelliten-gegen-propaganda-lehren-aus-dem-ukraine-krieg-wie-taiwan-eine-krisensichere-digitale-festung-errichtet/28826932.html.

[47] KITA, "미국·일본·호주, 해저케이블 협력 강화…중국 견제", https://kita.net/cmmrcInfo/cmmrcNews/cmmrcNews/cmmrcNewsDetail.do?pageIndex=1&nIndex=62931&sSiteid=2

고명현
외교안보센터

고명현 박사는 아산정책연구원의 선임연구위원이다. 고 박사는 외교안보 이슈에 대한 계량적 접근을 바탕으로 북한체제의 지속 가능성 및 장기 전략, 제재 및 수출통제, 사이버, 한반도 안보 환경 등을 연구한다. 최근 연구 저서로는 트럼프 행정부의 대북제재 변화를 분석한 "Not Under Pressure: How Pressure Leaked of North Korea Sanctions" (2020)와 러시아의 대북 석유 수출선을 파헤친 "The Rise of Phantom Traders: Russian Oil Exports to North Korea" (2018) 등이 있다. 고 박사는 미 컬럼비아 대학교 (Columbia University)에서 경제학 학사 (1999) 및 통계학 석사 (2001) 학위를 취득했으며, 미 랜드연구소 (RAND Corp.) 산하 대학원인 Pardee RAND Graduate School에서 정책분석학 박사 학위를 취득한 후 (2010) 미 캘리포니아 대학교 로스앤젤레스 (UCLA) 에서 박사후 연구원으로 재직했다. 2015년 뮌헨안보회의(MSC)의 '젊은 리더' (Young Leader)로 선출되었던 고명현 박사는 現 미국 신미국안보센터 (CNAS)와 영국 왕립합동군사연구소 (RUSI)의 객원연구위원이자 한국 국방부 자문위원이다.