해양안보 Maritime Security
제8권 제1호(통권 8호)

Vol. 8, No. 1, 2024
pp. 103-128

해저전 대응방안 연구: 해저케이블을 중심으로

조 성 진* · 임 수 훈**

◀ 국문 초록 ▶

노르트스트림 폭발, 발트해와 홍해에서의 해저케이블 훼손 사건은 전 세계적으로 해저전에 관한 관심을 불러일으키고 각국은 대응방안을 준비하고 있다. 하지만 한국은 해저케이블에 네트워크 대부분을 의존하고 북한과 주변국의 위협에 취약한 상황이지만 해저전(Seabed Warfare)이라는 용어조차 익숙하지 않다. 본 논문은 해저전의 정의와 특징, 각국의 현황을 분석하고 대응방안을 제시하는 국내 최초의 연구물이다. 해저전 대응을 위해 국제적으로 규칙기반의 질서를 공유하는 국가 간 소다자주의에 의한 협력체계 구축, 국내 관계 기관 및 업체와의 거버넌스 구축, 거부적 억제와 보복적 억제에 기초한 군사적 대응방안을 제시한다.

주제어 : 해저전, 해저케이블, 해저 인프라, 해저전 대응, 해양안보

* 해군 중령, 해군미래혁신연구단 작전능력연구담당. e-mail: jsjmoon@naver.com
** 해군 소령, 해군미래혁신연구단 해양전략연구담당. e-mail: keepship2@naver.com

Ⅰ. 서 론

이익을 얻고 부가가치가 창출되는 모든 것은 갈등과 위협의 대상이 된다. 영토와 자원은 전통적인 전쟁의 대상이었다. 오늘날 전쟁은 우주, 사이버, 전자기스펙트럼 영역까지 확대되었는데, 인간의 활동이 그 영역까지 다다르고 이익을 얻을 수 있기 때문이다. 인류의 생활에 점점 더 많은 영향을 미치고 있지만, 관심을 크게 받지 못하는 대상이 있다. 바로 해저(Seabed) 공간이다. 해저에서 심해자원을 채취하거나 파이프라인을 통해 석유나 천연가스를 운송할 수 있다. 또한 지식정보화 시대가 심화되어 데이터 사용이 폭발적으로 증가함에 따라 국가와 대륙 간 데이터를 이송하는 해저케이블(Submarine Cable)에 대한 의존도는 더욱 높아지고 있다. 이미 10여 년 전부터 서구 국가들에서는 이러한 해저 기간시설을 공격하고 보호하는 해저전(Seabed Warfare)에 관한 연구가 활발히 진행되고 있다.

2022년 9월 26일 러시아에서 독일로 이어지는 노르트스트림 천연가스 파이프라인이 폭발하며 천연가스가 누출되었고, 해저전에 관한 관심이 급증하게 되었다. 이어 2023년 10월 7~8일 또 다른 해저 파이프라인이 손상을 입었고 핀란드와 에스토니아를 잇는 해저케이블에도 손상이 발생하였다. 일부 서방 인사들은 근처에 러시아 군함이 있었다고 주장하였지만, 러시아는 오히려 미국, 영국, 우크라이나가 러시아를 차단하기 위해 사건을 저질렀다고 비난했다. 2024년 2월, 스웨덴은 조사결과 어떠한 증거도 발견할 수 없었다고 발표했으나, 독일은 미상의 잠수부가 폭발물을 파이프라인에 부착한 것으로 의심하며 계속 조사를 이어가고 있다.[1] 또한, 2021년 11월에는 노르웨이 해저 감시 센서용 케이블 4.3km가 절단되어 사라진 일이 발생했으며 2022년에도 같은 일이 여러 차례 더 발생하였다.[2] 2023년 12월에는 후티 반군이 홍해를 통과하는 해저케이블을 공격할 수 있다고 위협했고, 2024년 2월 26일 홍해를 지나는 총 16개의 해저케이블 중 4개가 손상을 입은 것으로 드러났다.[3] 그동안 이론적으로만 우려했던 해저전이 이제 현실로 다가온 것이다.

해저케이블과 같은 해저 인프라는 방어하기가 극도로 어렵고, 공격 주체를 신속하게 식별하기도 쉽지 않아 하이브리드 전쟁의 대상으로 활용하기가 쉽다.[4] 세계 각국

---

1) Johan Ahlander, "Sweden ends Nord Stream sabotage probe, hands evidence to Germany," *REUTERS*, 2024. 2. 8.

2) Nina Berglund, "Surveillance cables mysteriously cut," *NEWSinENGLISH*, 2017. 11. 7.

3) Brandon Vigliarolo, "Underwater cables in Red Sea damaged months after Houthis threatened to do just that," *The Register*, 2024. 2.27.

4) 하이브리드 전쟁은 여러 가지 복합적 성격을 갖고 있으며 공격의 주체, 대상, 방법, 의도, 배경, 결과 등 그 실상과 내용을 정확히 규정하기가 어렵다. 러시아는 크림반도 침공과 우크라이나 전쟁에서 군사적, 정치적, 외교적 수단을 동시에 사용하고, 사이버전, 정보전, 심리전, 정치전, 경제전, 대리전, 테러, 전복 등을 포함한 광범위한 비전통

은 노르트스트림 사건 이후 해저전에 대해 많은 관심을 가지고 연구하고 있다. 우리나라는 북한과의 분단으로 사실상의 섬나라이며, 인터넷 통신의 절대량을 해저케이블에 의존하고 있다. 하지만 우리나라에는 해저전이라는 용어 자체가 생소하고 관련 연구가 많지 않다. 또한, 해저케이블은 사이버안보 측면에서도 중요하다. 4차 산업혁명 시대의 심화로 정보통신 시스템의 마비는 국가 경제 전반을 직접적으로 위협할 수 있다.[5] 지금까지 사이버안보에 대한 논의는 주로 사이버 공간에서의 해킹과 같은 소프트웨어적 위협에 초점이 맞춰져 왔으며, 데이터의 직접적인 이동통로인 해저케이블 보호에 대한 논의는 부족하였다.

고명현, 임정희는 해저케이블에 대해 데이터 안보 관점에서 분석하고 복원력 강화와 이중화를 주장하였다.[6] 오일석은 해저케이블에 대한 위협을 국가안보 차원에서 다뤄야 하며 이를 위해 핵추진 잠수함 도입을 주장하였다.[7] 최일은 국내에서 최초로 해저전이라는 용어를 사용하며 해저전의 개념과 각국의 현황을 소개하였다.[8] 최현호는 최근 해저전의 주요 사례와 각국의 해저전 준비 현황을 분석하였다.[9] 고명현, 임정희, 오일석의 연구는 해저케이블 위협을 안보 차원에서 다뤄야 함을 제시했다는 점에서 의의가 있으나 해저전과 연결하지는 못했다. 최일과 최현호는 해저전을 소개하였으나 구체적인 대응방안 제시에는 이르지 못했다.

본 연구는 해저케이블에 대한 의존도와 위협이 동시에 증가하고 있고 해외에서 해저전에 대한 연구가 진행되고 있지만, 한국의 대응방안 연구는 미흡하다는 문제의식에서 출발한다. 본 연구는 해저전 대상 중 우리나라와 관련이 높은 해저케이블을 주로 분석한다. 본 연구의 연구 질문은 다음과 같다. 해저전은 무엇이고 왜 중요한가? 주요 국가들은 해저전을 어떻게 준비하고 있는가? 해저전에 대응하고, 특히 해저케이블을 보호하기 위해 무엇을 해야 하는가? 해저전은 그 주체가 불분명하고, 증거 확보가 어려우며 대응이 어려운 하이브리드적 위협이다. 특히 해저케이블이 영해뿐만 아니라 공해상에 광범위하게 존재하므로 여러 국가와 행위자에 의한 종합적인 대응이 필요하다. 따라서 본 논문에서는 대응방안을 국제적, 국내적, 군사적 차원으로 나눠

적 전쟁방식을 동시에 사용하였다. 하이브리드 위협에 대한 내용은 온대원, "하이브리드 안보위협에 대한 EU의 대응정책," 『EU연구』제59호, 한국외국어대학교 EU연구소, 2021. 참조.

5) 심세현, "디지털 기술의 발전과 사이버안보 위협," 『국가와 정치』제29집 1호, 동아시아연구소, 2023, pp.204-210.

6) 고명현·임정희, "해저케이블망과 데이터 안보," 이슈브리프 2022-35호, 아산정책연구원, 2022.12.29.

7) 오일석, "해저케이블을 통해 전송되는 정보와 데이터의 안정성 확보 방안," 이슈브리프 330호, 국가안보전략연구원, 2022. 2. 8.

8) 최일, "해저전," SPNNews, 2023.10.30.

9) 최현호, "해저 인프라 보호 강조되는 해저전: 기뢰전에서 해저케이블 보호까지 확대되는 해저 작전," 『국방과 기술』 539호, 한국방위산업진흥회, 2024. pp.100-107.

제시할 예정이다. 본 논문의 가치는 국내에서 최초로 해저전 대응방안을 연구한 논문으로서 향후 해저전에 대응하기 위한 기초 연구자료를 제공하고, 대응 정책과 전략 수립에 기여한다는데 있다.

Ⅱ. 해저전이란

1. 해저케이블의 중요성과 해저전 정의

해저에 대해서는 아직 많이 알려지지 않았다. 바다의 평균 수심은 3,800m이며 해저면의 수심은 일정하지 않고 연속성을 보여주지도 않는다. 전체 해저면의 20%만이 측심기로 정확하게 측정되었고, 미터 단위로 정밀하게 밝혀진 해저면은 2%에 불과하다. 지표면과 달리 항공관측이나 위성을 통해 정확하게 해저면을 측정할 수 없고, 선박에 설치된 음향센서를 이용하여 측정해야 하므로 정확성을 확보하기도 어렵다.

통상 심해는 빛이 거의 닿지 않아 광합성 작용이 일어나지 않는 수심 200m 이상으로 정의하며 전체 해양의 95%의 용적을 차지한다.[10] 심해에서는 수심에 비례하여 강한 수압이 작용해 인간이 활동하기란 어려운 일이었다. 과거에 심해에서 활동하기 위해서는 높은 수준의 기술과 자본이 요구되었다. 강대국이나 해양 석유 시추를 전문으로 하는 몇 개의 대형 석유 회사만 이러한 기술을 가지고 있었다. 하지만 기술의 발전과 보편화로 해저 탐사 기술은 더 확산되었다. 일례로 마이크로소프트의 공동 창업자인 폴 앨런(Paul Allen)은 민간 자본과 기술을 활용해 필리핀해의 수심 5,500m의 수심에서 2차 세계대전에서 침몰한 인디애나폴리스함을 발견하였다.[11] 과거에는 기술을 선도하는 조직이나 국가가 폐쇄적으로 관리하여 기술에 접근이 쉽지 않았으나 현대 정보통신 기술의 확산으로 기술과 지식에 대한 접근성은 증가하였다.[12] 즉, 해저전 능력을 확보하고 활용하는 것이 점점 더 쉬워지고 있어, 개발도상국, 혹은 비국가 행위자에 의한 해저전 위협이 증가하고 있다.

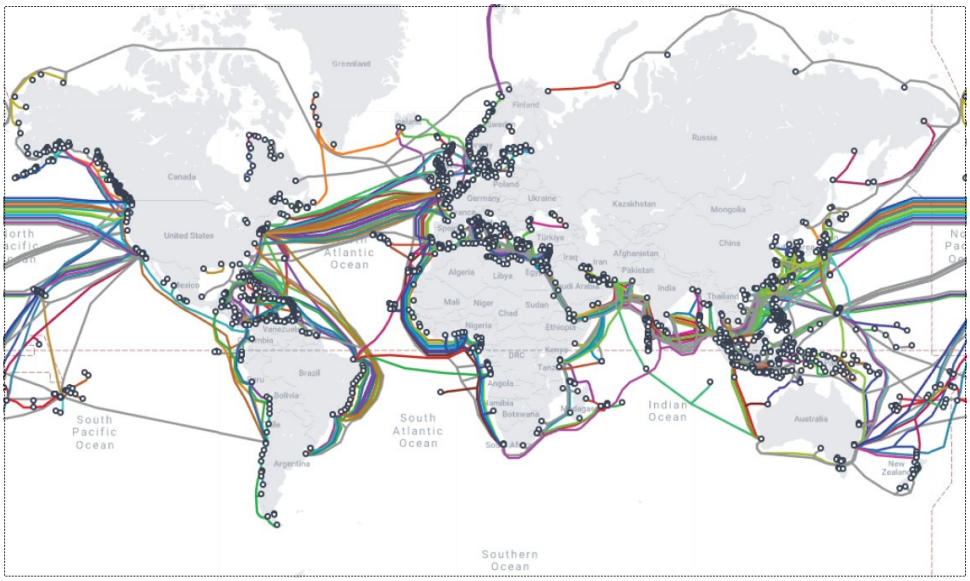
---

10) https://oceanexplorer.noaa.gov/facts/deep-ocean.html(검색일자: 2024. 1.15.).

11) Ben Werner, "Billionaire Paul Allen Finds Lost World War II Cruiser USS Indianapolis in the Philippine Sea," *USNI News*, 2017. 8.19.

12) Insightunboxed, "Technology Proliferation: Threat or Opportunity?," *Insightunboxed*, 2019. 5.14.

[그림 1] 세계 해저케이블 지도



* 출처: Submarine Cable Map

해저에 설치된 에너지 파이프라인, 전력선, 해저케이블 등 해저 인프라는 우리 생활에 많은 영향을 미치고 있다. 특히, 이 논문의 분석 대상인 해저케이블에 대한 의존도는 폭발적으로 증가하고 있으며 우리의 삶을 근본적으로 바꾸고 있다. 4차 산업혁명의 대표 기술인 AI, 클라우드, IoT, 증강현실, 메타버스 등은 모두 네트워크를 기반으로 하고 있다. 전 세계 데이터의 99%가 해저케이블을 통해 이동하고 있으며, 매일 10조 달러 이상의 금융 송금이 이루어지고 있다.[13] 〈그림 1〉은 세계 각국을 이어주는 해저케이블 현황을 나타낸다.

텔레지오그래피(Telegeography)에 따르면, 국제 인터넷 이용 용량은 2019년 450Tbps에서 2022년 997Tbps로 폭증했다.[14] 2030년까지 네트워크 트래픽은 연평균 22~50%의 성장률을 기록할 것으로 예상된다.[15] 우리나라와 연결된 해저케이블의 전체 용량은 2022년 200Tbps를 돌파했다.[16] 최근에는 구글, 아마존, 마이크

13) Nishant Batra, "Technology Strategy 2030: Nokia's guide to the emerging technologies that are radically changing our world," NOKIA, 2023. 11. 8. https://www.nokia.com/about-us/newsroom/articles/introducing-nokias-technology-strategy-2030/(검색일자: 2024. 1.10.).

14) Telegeography, The State of the Network, 2023. p.10. https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2023.pdf(검색일자: 2024. 1.10.).

15) NOKIA, Global Network Traffic 2030 Report, 2023. p.10. https://onestore.nokia.com/asset/213660(검색일자: 2024. 1.10).

16) 차종환, "국경 없는 데이터 고속도로, '해저케이블' 관심집중," 정보통신신문, 2023. 9.22.

로소프트, 메타 등 이른바 세계적인 빅테크 기업들이 자체 해저케이블을 직접 부설하고 있다.[17] 미래 4차 산업혁명 시대에는 안정적인 네트워크가 필수적이므로 빅테크 기업들이 독자적인 망 구성에 나선 것이다.

한편 해저전에 대한 우리나라에서 명확한 정의는 없다. 미국은 2023년 12월에 발간된 『합동해양작전(Joint Maritime Ops)』교범에서 해양통제의 대상 영역에 공중, 수상에 이어 해저를 포함하였다.(Sea control includes the airspace above the surface and the water volume and seabed below.)[18] 또한 해저전(Subsea or Seabed Warfare)을 대잠전(Anti Submarine Warfare), 기뢰전(Mine Warfare)과 더불어 수중전(Under Sea Warfare)을 구성하는 작전 중 하나로 설명하고 있다.[19] 미국은 해저전에 대해 명확히 정의하지 않고, 해저전은 잠수함이나 기뢰 이외의 시스템(UUV, ROV, 해저 시스템)을 이용하여 수중영역이나 해저에서 효과를 창출한다고 설명하였다.[20] 프랑스는 해저전을 자체적으로 또는 네트워크 내에서 작동할 수 있는 시스템을 포함하는 해저에서 수행되는 모든 작전으로 정의한다.[21] 최일은 적국의 해저 자산을 사전 탐지해서 필요시 공격하며, 자국의 해양자산을 보호하고 방어하기 위해 수중 해저에서 이루어지는 작전으로 정의한다.[22]

이상에서 살펴본 바와 같이 해저전에 대한 충분한 논의와 정의는 이루어지지 않았다. 미국이 교범에서 명확히 명시하지 않은 것처럼 해저전이 벌어지는 영역, 그리고 기존에 수중에서 벌어졌던 대잠전과 기뢰전과의 관계에 관한 추가적인 연구가 필요하다. 아직 국내에서는 해저전에 대한 공식적인 정의는 없지만 본 연구에서 해저전은 “수중 및 해저에서 해저 파이프라인, 해저케이블, 해저 자원 등 해저 자산을 공격하고 보호하기 위해 수행하는 대잠전과 기뢰전을 제외한 모든 작전”으로 정의한다.

2. 국제법과 해저전의 특징

해저케이블과 같은 해저 자산에 대한 의존은 급증하고 있지만 이를 위한 국제법과 관련 협약들은 미비한 실정이다.[23] 해저케이블에 대한 최초의 국제 협약은 1884년

---

17) Christopher Mims, “Google, Amazon, Meta and Microsoft Weave a Fiber-Optic Web of Power,” *The Wall Street Journal*, 2022. 1.15.

18) JCS, *Joint Maritime Ops*(Washington DC: Joint Chief of Staff, 2023), p.I-4.

19) 미국은 다른 나라와는 다르게 해저전에 대해 Seabed Warfare와 Subsea Warfare라는 용어를 동시에 사용하고 있는데 왜 그런지에 대한 설명은 없다. 해저전이 벌어지는 공간이 해저면 뿐만 아니라 해저와 수면상의 공간에서도 벌어질 수 있고, 개념 정립이 명확히 되지 않은 상황이라 두 용어를 동시에 사용하는 것으로 판단된다.

20) JCS, *Joint Maritime Ops*, pp.I-9~V-3.

21) Ministère des Armées, *French Seabed Warfare*(Paris: Ministère des Armées, 2022). p.9.

22) 최일, “해저전,” SPNNews, 2023.10.30.

파리에서 체결된 「해저 전신 케이블 보호를 위한 협약(Convention for the Protection of Submarine Telegraph Cables)」이다. 이 협약은 현재도 발효 중이며 유엔해양법협약의 해저케이블 분야의 기초가 되었다.[24] 국제 사회는 2010년 12월 7일 유엔 총회에서 「해양과 해양법에 관한 결의」에서 해저케이블을 중요한 통신시설(critical communications infrastructure)로 인정하였다. 해저케이블을 보호하기 위한 국제법은 유엔해양법협약에 찾아볼 수 있다.[25] 유엔해양법협약 113조에는 해저케이블을 고의나 과실로 파괴하거나 훼손하는 자국 국적 선박 또는 자국 관할권 내에 존재하는 사람을 처벌하기 위한 입법 의무를 부과하고 있다. 114조에는 해저케이블 부설이나 수리 도중 다른 전선을 파괴하거나 훼손한 경우 수리비용을 부담하기 위한 입법 의무를 부과하고 있다. 하지만 많은 국가에서 해저케이블 보호와 관련한 국내 입법이 미비한 상황이며, 외국 국적의 선박이나 인원에 의한 피해에 대해서는 관할권을 갖지 못한다. 즉, 가상 적국이나 단체에 의한 의도적인 해저케이블 공격행위에 대해서 금전적 책임이나 국가책임을 다루고 있는 국제법이 존재하지 않는 것이다. 이외에도 해저케이블 훼손은 사안에 따라 유엔헌장 51조인 무력공격에 해당할 수 있다는 주장도 제기되고 있다. 해저케이블 손상으로 인한 파급력은 계속 증가함에 따라 무력공격의 판단 기준인 '규모와 효과(Scale and Effect)' 요건을 충족하기에[26] 해저케이블 손상시 개전 사유로 활용될 개연성도 존재한다는 것이다.

해저전은 우주전과 사이버전의 작전환경과 유사하다. 첫째, 민간분야와 군사분야에서 모두 사용되는 기술을 사용한다. 해저자원 채취 및 이송, 해저케이블을 통한 데이터 이송을 위한 기술은 고스란히 해저에서의 군사작전에 활용된다. 둘째, 인간이 직접 거주하지 않는 공간에서 행위가 발생한다. 사이버 공간에서는 디지털 신호에 의해, 우주와 해저에서는 로봇과 같은 기계를 통해 대부분의 행위가 이루어진다. 심해에서는 주로 ROV(Remotely Operated Vehicle)와 AUV(Autonomous Underwater Vehicle)와 같은 무인잠수정(UUV: Unmanned Underwater Vehicle)이 주로 사용된다.[27] 셋째, 실시간 모니터링이 어려워 쉽게 은폐할 수 있고 행위자를 특정하기도

---

23) Tara Davenport, "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis," *Cath. U. J. L. & Tech* Vol.24, 2015, pp.108-109.

24) Douglas R. Burnett, "Submarine Cable Security and International Law," *International Law Studies*, Vol.97, 2021, pp.1670-1671.

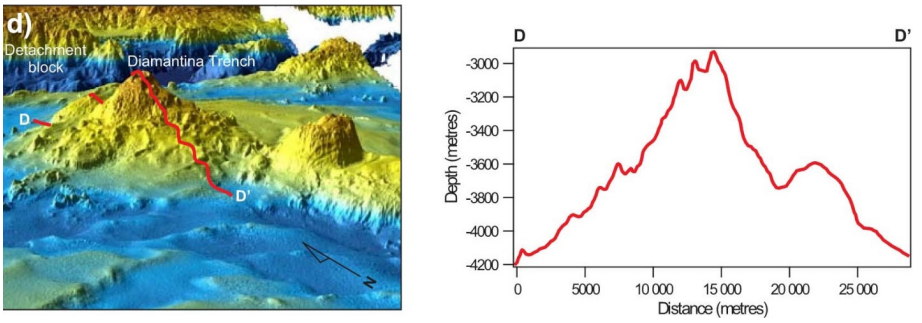
25) 김채형, "해저케이블 부설과 이용에 관한 국제 사회의 법적 체제," 『해사법연구』제29권 제1호, 한국해사법학회, 2017, pp.41-68.

26) 유준구, "사이버작전 시 유엔해양법 원칙 적용의 현안과 과제," 『IFANS 주요국제문제 분석』, 2022-45호, 국립외교원 외교안보연구소, 2022, p.13.

27) 사용자와 유선으로 물리적으로 연결되어 조종하는 형태를 ROV, 별도의 연결선 없이 주어진 임무를 프로그램에 따라 자율적으로 수행하는 형태를 AUV라 하며, 이를 통칭하여 UUV라 한다. ROV와 AUV는 별도 국문

어렵다.[28] 해저전은 이러한 환경으로 인해 행위자를 특정하기도 어렵고 공공재인 공해상에서 주로 벌어지기 때문에 하이브리드 전략을 전개하기에 적합하다. 특히, 해저전은 평소에 해저 환경에 대한 장시간의 사전조사가 필요하다. 〈그림 2〉는 인도양 지아만티나 해구(Diamantina Trench)의 지형을 조사한 결과다. 조사한 구간의 길이는 약 30km인데 수심은 3,000m에서 4,200m로 매우 다양하다. 따라서 평소에 충분한 사전조사가 이루어지지 않으면, 실제 해저에서 사건이 발생했을 때 신속한 대응이 어렵다.

〈그림 2〉 인도양 지아만티나 해구 지형



* 출처: CIMSEC

3. 한국에서 해저전의 의미와 취약성

우리나라는 IT 강국의 명성에 걸맞게 사회/경제/행정/생활 등 전 분야에 걸쳐 정보통신 네트워크에 의존하고 있다. 국내 전체 가구의 인터넷 접속률은 99.96%이며, 3세 이상 국민의 인터넷 이용자 수는 93%, 인터넷 뱅킹 이용률은 79.2%에 달한다. 그 외 주거 편의시설, 교통, 교육, 커뮤니케이션 등 우리 생활 전 분야는 네트워크에 밀접하게 연결되어 있다.[29] 이 외에 정부 기관의 서비스와 산업시설의 업무체계는 대부분 네트워크를 통해 연결된다.

현재 한국에 설치된 해저케이블 중 해외로 연결되는 것은 총 11개이며, 세부 현황은 〈표 1〉과 같다. 이 케이블은 부산, 거제, 태안에 있는 국제 육양국을 통해 해외와 연결된다. 2018년에 완공된 NCP(New Cross Pacific)는 한국과 미국을 직결하는

명칭없이 영문을 그대로 쓰므로 본 논문에서도 동일하게 사용한다. 고성협 외, "만타형 무인 잠수정의 개발과 실해역 성능시험," Journal of the Korean Society of Marine Engineering, Vol.37, No.6, 한국마린엔지니어링학회, 2013, pp.644-652.

28) Ministère des Armées, *French Seabed Warfare*, pp.20-21.

29) 한국지능정보사회진흥원, 『2022 한국인터넷 백서』(대구: 한국지능정보사회원, 2023), pp.12-20.

케이블로써 마이크로소프트가 주도하여 KT, Softbank Telecom, China Telecom, China Mobile, China Unicom, 중화통신 등이 참여하는 컨소시엄 형태로 운영된다.[30]

한국의 해저케이블은 질과 양에서 모두 취약한 상황이며, 대부분 일본 등 타국을 경유해 통신을 받고 있다. 회선의 공유는 그만큼 도청과 데이터 탈취의 위험이 있다. 일본과의 해저케이블은 지진 등으로 인해 환경적으로 취약하고, 중국·대만과 연결되는 해저케이블은 지정학적 리스크를 안고 있다. 또한, 대만은 총 15개의 해저케이블을 보유했지만, 한국의 해저케이블은 11개에 불과하다. 한국 해저케이블에 있어 가장 취약한 것은 해저케이블이 지상 통신망과 연결되는 지점인 국제 육양국(Cable Landing Station)의 위치다. 〈표 1〉과 〈그림 3〉에서 알 수 있듯이 총 11개의 육양국 중 태안, 포항 각 1개소를 제외한 나머지 회선이 전부 부산과 거제 육양국에 몰려 있다.[31] 만약 부산과 거제 앞바다에 집중적으로 위치한 해저케이블이나 육양국이 공격받는다면 전체 회선의 72%를 한꺼번에 상실한 우려가 있다.

〈표 1〉 한국의 해외 연결 케이블 현황

명칭	건설구간	길이 (Km)	개통 연도	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
APVN2	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	SK Broadband	부산
Bridge One	한국-일본	330	2025	DCT Cable	포항

* 출처: 고명현·임정희, "해저케이블망과 데이터 안보," p.8.

30) 고명현·임정희, "해저케이블과 데이터 안보," pp.7-8.

31) 위의 글, pp.9-13.

[그림 3] 한국의 해저케이블

* 출처: Submarine Cable Map

해저케이블이 손상되면 구글 등 해외 사이트 접속이 불가해질 뿐만 아니라 국가기관과 금융기관 전산망 마비로 얼마만큼의 손실을 볼지 예상할 수조차 없다고 전문가들은 경고한다. 또한, 끊어진 해저케이블은 복구도 쉽지 않다. 전 세계 해저케이블은 천재지변 등의 원인으로 2주에 한 번꼴로 훼손이 발생하는데, 이를 복구하려면 빛의 파동을 활용해 결함 부분을 찾고, 복구 장비와 인력이 해당 위치로 이동하고, 수심에 따라 로봇이나 갈고리 등을 이용해 케이블을 회수하는 과정을 거쳐야 한다. 빨라도 수주 이상이 소요된다.[32] 전체 케이블이 파손되지 않고 일부 케이블이 파손되더라도 문제가 된다. 여러 회선을 통해 나누어 담당하던 인터넷 트래픽이 일부 온전한 케이블에 몰리면서 전체 회선의 속도 저하가 발생하게 된다. 실제로 2022년에 베트남 해저케이블 중 4개의 케이블이 고장나면서 인터넷 사용에 큰 혼란이 발생했다.[33]

32) 변휘, "'초연결 세계' 무너뜨린 해저화산…한국인터넷은 안전할까," 머니투데이, 2022. 1.22.
33) 김범수, "베트남, 인터넷 개선되나…'고장' 해저케이블 5개 중 1개 수리, 연합뉴스, 2023. 4.28.

Ⅲ. 각국의 해저전 현황

해저케이블은 무선 통신의 수단으로 활용된 이후 공격의 대상이 되어왔다. 1898년 미국-스페인 전쟁에서 미국은 스페인, 필리핀, 쿠바 사이의 해저 전신 케이블을 절단했다. 1차 세계대전 중 독일 잠수함 U-151은 뉴욕과 영국을 연결하는 해저 전신 케이블을 절단했고 영국 역시 양차 세계대전에서 독일과 아메리카 대륙을 연결하는 전신 케이블을 절단했다.[34] 제2차 세계대전 말기인 1945년 7월, 영국 해군은 베트남 인근에 일본군이 부설한 해저 통신케이블을 끊어 일본군의 통신을 방해했다.

냉전 시기 해저전은 일부 강대국 간의 대결이었으며, 첩보전의 한 분야였다. 1970년대 미 해군은 국가보안국(NSA), 중앙정보국(CIA)과 영국과 공조하여 '아이비 벨 작전(Operation Ivy Bell)'을 수행했다. 이 작전은 캄차카반도에 있는 페트로파블롭스크 해군기지와 블라디보스토크 함대사령부를 연결하는 소련의 오호츠크해 해저 통신케이블에 특수 잠수함을 이용하여 도청장치를 설치하는 것이었다.[35]

해저전에 있어 세계 최고수준의 능력을 갖추고 있는 나라는 러시아와 중국이다. 러시아는 해저전과 정보작전을 위한 특수임무 잠수함 부대를 가진 유일한 국가다. 러시아의 해저전은 군사정보기관인 GRU와 심해연구본부인 GUGI(Glavnoye Upravleniye Glubokovodnykh Issledovaniy)에 의해 수행되는 것으로 알려져있다. 1965년에 설립된 심해연구본부는 군조직은 아니지만 해저전의 핵심기관이며 전력과 병력은 러시아 해군으로 구성되어 있다.[36] 심해연구본부는 핵잠수함을 개조한 잠수모선인 Belgorod와 BS-64 Podmoskovye를 보유하고 있다. Paltus, X-Ray, Kashalot, Losharik 등 4척의 특수임무 잠수함도 보유하고 있는데 선체가 티타늄으로 제작되어 극한의 수심에서도 작동하는 것으로 알려져 있다. 특히, Losharik(로샤리크)함은 소형 핵추진 심해잠수함으로 2,500m 해저까지 잠항이 가능하며, 통신 케이블 도청이나 절단 같은 특수작전을 수행할 수 있다. 또한, Yantar급 정보함 3척도 타국의 해저 통신 케이블 현황을 조사하는 목적으로 운용하고 있는데 6,000m 수심까지 운용 가능한 Pr18610 심해 잠수정과 다양한 ROV와 AUV를 탑재한다.[37]

---

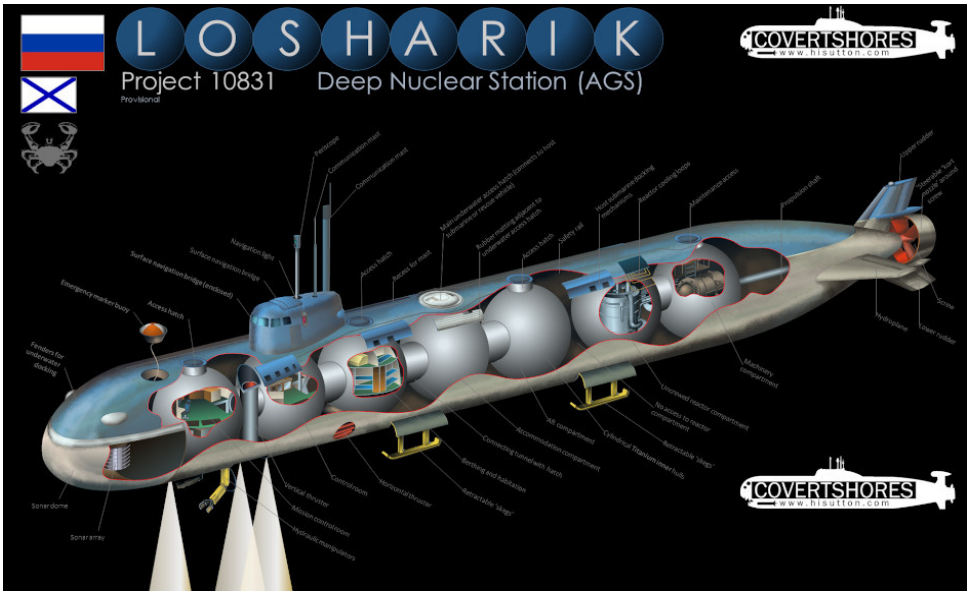
34) Douglas R. Burnett, "Repairing Submarine Cables Is a Wartime Necessity," *Proceedings*, Vol.148/10/1,436, 2022.10.

35) Marcia Wendorf, "Operation Ivy Bells: The U.S. Top-Secret Program That Wiretapped a Soviet Undersea Cable," *Interesting Engineering*, 2022. 1. 3.

36) H. I. Sutton, "Russia's Growing Secret Submarine Fleet Key to Moscow's Undersea Future," *USNI News*, 2021.11.30.

37) Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," *RUSI*, 2023. 5.25.

〈그림 4〉 러시아의 Losharik 핵추진 심해 잠수함



* 출처: Corvert Shores

중국은 5년마다 경제사회발전과 장기 목표를 위한 계획인 5개년 규획을 발표한다. 제13차(2016~2020)와 제14차(2021~2025) 5개년 규획에서 모두 심해의 중요성에 대해 언급했다. 『과학기술혁신계획 2030』에서 심해탐사와 기술 연구를 위한 심해 우주정거장(Deep Sea Space Station) 개념을 제시했다.[38] 또한, 해저 만리장성(Undersea Great wall) 계획을 진행하여 중국 연근해와 남중국해에 수중 감시를 위한 수중 센서 및 인프라 네트워크를 구축했다. 이는 미국 등 적대적인 국가의 잠수함 활동을 감시하고 대응하기 위함이며, 이렇게 구축된 수중 네트워크는 해저전 능력으로 이어질 가능성이 높다. 중국은 민간기업과 대학이 수준 높은 무인잠수정들을 개발하고 있는데 이미 2016년부터 인도양과 남중국해에 무인잠수정을 운용하여 정보를 수집하고 있다. 무인잠수정 Haidou-1은 10,908m의 수심의 잠수에 성공하였고 수중글라이더 Haiyan은 남중국해를 141일 동안 3,619.6km를 항해하는 기록을 세웠다.[39] 또한, 중국이 대만을 고립시키기 위해 대만의 해저케이블을 차단할 가능성이 있다. 실제로 2023년에는 중국에서 불과 20km 떨어진 대만 마주(Matsu) 섬과 대만을 연결하는 해저 통신 케이블이 중국 선박에 의해 파손되어 약 2달 동안 주민 생활

38) 中国国务院, "十三五国家科技创新规划的通知," https://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm(검색일: 2024. 2.23.).

39) Prakash Panneerselvam, "Unmannes Systems in China's Maritime 'Gray Zone Operations'," *The Diplomat*, 2023. 1.23.

이 마비되었는데 중국은 비의도적인 사고라고 주장하였다.[40]

미국은 냉전 시기부터 해저전에 있어 탄탄한 경험을 보유하고 있다. 시울프급 핵잠수함인 지미 카터함(USS Jimmy Carter)은 동형함보다 길이가 30m 더 길다. 늘어난 부분에는 특수작전용 ROV를 적재하고, 특수부대를 운용할 수 있다.[41] 시울프급의 후속함인 버지니아급 핵잠수함 1척을 해저전용으로 추가로 건조하고 있다. 세부 성능은 알려지지 않았지만, ROV, 혹은 특수작전 잠수정을 탑재할 것으로 추정된다.[42] 미국은 기존의 수중 음향탐지시스템인 SOSUS를 통합해저탐지시스템(Integrated Undersea Surveillance System)으로 업그레이드하였다. 또한, 전시 미국 본토의 해저케이블을 수리하기 위한 해저케이블 안보 함대(Cable Security Fleet)를 2021년에 창설하였다. 이 함대는 미국 국적의 해저케이블 수리 선박 2척으로 구성되어, 전시 등 비상상황이 선포되면 미국 정부에 동원되어 최우선으로 해저케이블 수리작업을 실시한다.[43]

프랑스와 영국을 위시한 유럽 국가들은 노르트스트림 해저 파이프 폭파 사건 이후 해저전 위협을 심각하게 인식하고 대응 역량을 키우고 있다. 프랑스는 2022년 2월 『해저전 전략(Seabed Warfare Strategy)』을 발표하였다. 프랑스는 해저에서 점점 더 많은 분쟁이 발생할 것으로 예측하고 있다. 국익과 안보전략에 있어 중요한 가치를 지닐 것으로 판단하고 수심 6,000m까지 작전할 수 있는 해저전 능력을 갖추는 것을 목표로 명시하고 있다.[44]

영국은 2006년에 발간된 "해저케이블 기술 개요-An Overview of the Submarine Cable Technology"라는 보고서에서 해저케이블 안보에 대해 최초로 언급하였다.[45] 영국 해군의 10가지 임무 중 하나로 해저에서의 국가 중요 기반시설을 보호하는 것을 명시하였으며, 특히 러시아가 가장 위협적이라고 인식하고 있다.[46] 이에 대응하기 위해 영국은 새로운 해양감시 선박(Multi Role Ocean Surveillance Ship) 2척을

---

40) Venus Upadhayaya, "Seabed Warfare is New Domain in CCP's Quest to Dominate the Indo-Pacific," *The EPOCH TIMES*, 2023.10.13.

41) Peter Suciu, "USS Jimmy Carter: The Navy Has a Spy Submarine That Can't Be Matched," *The National Interest*, 2023.11.23.

42) H. I. Sutton, "U.S. Navy To Get New Unique Submarine: Virginia SSW," *Naval News*, 2023. 4.20.

43) Douglas R. Burnett, "Repairing Submarine Cables Is a Wartime Necessity"

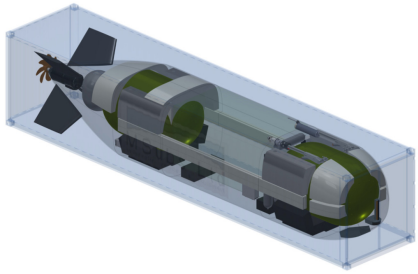
44) Ministère des Armées, *French Seabed Warfare*, pp.8-11.

45) CPNI, "An Overview of the Use of Submarine Cable Technology by UK PLC," https://cyberwar.nl/d/20060300_Submarine-cables_CPNI-UK.pdf(검색일자: 2024. 2.21.).

46) House of Commons, "We're going to need a bigger Navy," https://committees.parliament.uk/committee/24/defence-committee/news/159793/were-going-to-need-a-bigger-navy/(검색일자: 2024. 2.21.).

도입하고 있는데 첫 번째 함정인 RFA Proteus함이 2023년 10월에 취역했다.[47] 또한, 기존 AUV보다 훨씬 큰 12m급의 Cetus를 도입할 예정인데 컨테이너 내부에 실려 세계 어디든 신속하게 전개할 수 있고 배터리로 구동되며 한번 항해에 최대 1,000NM(1,852km)를 항해할 수 있는 것으로 알려졌다.[48]

[그림 5] 영국의 RFA Proteus함(좌)과 Cetus 잠수정(우)



* 출처: Naval Technology

해저전에 있어 중국과 러시아 등 권위주의 국가들은 주로 공세적인 방안을 준비하고 있지만, 미국, 영국, 프랑스 등 민주주의 국가들은 표면적으로 중·러의 공세에 대한 대응에 중점을 두는 모양새다. 중국과 러시아 등 이른바 수정주의 국가는 현재의 국제질서를 재편하는 것이 목적이다. 이 과정에서 투명하고 적법한 내부 의사결정 과정이나 국제법은 중요하지 않다. 특히, 공해상 수중에서 벌어지는 일은 실시간으로 파악하고 대응하기도 힘들며, 증거조차 남지 않는다. 최근 노르트스트림 가스관 폭발 사고나 대만 마주섬 해저케이블 절단 사건 등을 고려시 중국과 러시아가 유사시 해저케이블을 은밀히 공격할 가능성은 배제할 수 없다. 반면 민주주의 국가들은 현재의 규칙기반의 질서(Rule Based Order)를 중시하며 국제질서에 반하는 정책을 공공연하게 내세울 수 없다. 권위주의와 민주주의 국가들이 국제문제에 대결하는 양상이 해저전에서도 동일하게 나타나고 있는 것이다.

우리나라는 해저전에 있어 북한과 주변국으로 인한 위협 요인을 모두 갖고 있다. 북한은 최근 러시아와의 군사협력 관계를 급속도로 증진하고 있다. 러시아-우크라이나 전쟁이 2년이 지남에 따라 러시아는 포탄 등 부족한 군수물자를 북한으로부터 도입하였다. 북한은 그 대가로 식량과 첨단 군사기술을 러시아로부터 제공받았다.[49] 전

47) Louisa Brooke-Holland, "Seabed warfare: Protecting the UK's undersea infrastructure," *House of Commons Library*, 2023. 5.24.

48) Andrew Salerno-Garthwaite, "Seabed warfare is a 'real and present threat'," *Naval Technology*, 2022.12.20.

문가들은 북한이 주로 미사일, 인공위성, 항공기 기술을 받았을 것으로 예상하지만, 러시아의 해저전 공격 기술을 받았을 가능성도 배제할 수 없다. 한국은 정보통신 네트워크 의존도가 높고, 해저전은 사회경제적으로 높은 혼란을 초래할 수 있을 뿐만 아니라 즉각적인 원인 규명과 대처가 어려워, 북한 입장에서 선택하기 매우 좋은 군사적 도발 카드다. 육상에 설치된 육양국이나 통신네트워크 시설을 공격하는 것은 더 쉽고 비용도 적게 들지만 증거가 남고, 방어로 인해 공격 성공률이 낮으며, 영토를 직접 공격하는 것이므로 사실상 전쟁행위와 같다. 따라서 북한이 한국의 정보통신 기반 시설을 물리적으로 은밀하게 공격한다면 해저케이블을 대상으로 삼을 가능성이 크다.

또한 중국-대만과의 갈등 상황에서 한국도 피해를 볼 수 있다. 중국은 대만을 고립시키려 노력하고 있는데 전문가들은 중국이 대만의 해저케이블을 차단할 수도 있음을 경고하고 있다.[50] 해외와 연결된 한국의 해저케이블 11개 중 9개가 대만과 연결되어 있어 중국이 대만의 해저케이블을 공격하면 한국도 피해를 입을 수 밖에 없다.

Ⅳ. 해저전 대응 방안

1. 국제적 대응-소다자주의에 의한 협력체계 구축

해저케이블은 여러 나라와 연관되어 있다. 케이블 하나가 최소 2개국 이상을 통과하고 있고 건설할 때도 여러 나라가 공동으로 컨소시엄을 구성하여 설치하고 유지보수를 진행하는 사례가 대부분이다.[51] 따라서 해저 인프라에 대한 위협 대응에는 여러 나라의 협력이 요구되므로 소다자주의(Mini-multilateralism)에 의한 대응이 필수적이다.[52]

---

49) Christy Lee, "North Korean Missiles Used by Russia Against Ukraine Are Products of Sanction Loopholes," *VOA*, 2024. 2.27.

50) Venus Upadhayaya, "Seabed Warfare is New Domain in CCP's Quest to Dominate the Indo-Pacific," *The EPOCH TIMES*, 2023.10.13.

51) 각국 주요 통신사업자들은 아시아태평양, 북미, 대서양 등 지역별로 협정을 체결해 유지보수를 진행한다. 일례로 아시아태평양지역은 한국의 KT, 미국 AT&T, 일본 KDDI, 중국 차이나텔레콤 등이 컨소시엄을 구성해 5년 단위로 경쟁 입찰을 통해 유지보수 사업자를 선정한다. 2023년에는 우리나라의 LS 마린솔루션이 유지보수 사업자로 선정되었다. 한지연, "LS마린솔루션, 아태 해저케이블 유지보수 맡는다…年 130억 수익," 머니투데이, 2023. 9. 8.

52) 해저케이블을 보호하기 위한 대표적인 국제기구인 국제케이블 보호 위원회(ICPC: International Cable Protection Committee)라는 조직이 1958년에 설립되었다. 이 기구는 2023년 기준 70개 국가 200개 이상의 기업/단체가 회원으로 가입되어 있으며, 주목적은 해저케이블 관련 기술, 법률 및 정보를 교환하기 위함이다. 하지만 이 기구는 비공인 국제기구로서 의도적인 해저케이블 훼손과 같은 공격행위에 구체적인 책임을 묻기에는 한계가 있다. 자세한 사항은 https://www.iscpc.org/ 참조.

미국, 일본, 호주, 인도로 이루어진 QUAD 국가들은 해저케이블 보호를 위한 협의체를 구성했다. 2023년 5월 20일 정상회담 후 발표된 공동 성명에 인도태평양에서의 해저케이블망 보호에 관한 협의체(Quad Partnership for Cable Connectivity and Resilience) 관련 내용이 포함되었다.[53] 이 협의체의 목적은 QUAD 국가들의 전문 지식을 활용하여 인도 태평양에서의 해저케이블 보호를 강화하는 것과 해저케이블 분야에 중국의 영향력을 견제하는 것이다. QUAD 국가들은 중국의 해저케이블 회사가 미크로네시아 국가들에 해저케이블을 공급하는 것을 차단하기 위해 이들 국가에 자금을 지원하기로 합의하였다.[54]

한편, NATO는 2023년 2월 NATO 본부에 해저 파이프라인과 해저케이블을 보호하기 위한 해저 기반시설 협조실(Undersea Infrastructure Coordination Cell)을 창설했다.[55] 이는 각국의 군사와 민간 해저산업계의 노력을 하나로 모으고, 해저 인프라에 대한 위협을 공동으로 감지하고 대응하기 위함이다. 또한, 같은 해 7월에는 NATO 연합 해양사령부(MARCOM) 내에 해저 인프라 보호를 위한 해양 센터를 설립하기로 합의했다.[56]

우리나라의 해저케이블은 일본, 중국, 대만 등 주변국과 연결되어 있어 주변 국가와의 협력이 필수적이다. 특히, 규칙기반의 해양질서를 공유하고 있는 미국, 일본, 대만, 호주와의 협력이 필요하다. QUAD와 NATO가 국가 간 협의체를 구성하는 것처럼 주변국 정부와 민간산업계가 모두 참여하는 다양한 협의체에 참가해야 한다. 협의체를 통해 해저케이블에 관한 정보를 공유하고, 공동 감시방안을 구축하고 대응방안을 공유해야 한다. 국제공동 회의와 연합 훈련에 정부, 군, 산업체가 참여하고, 해저케이블 위협에 대해 각국의 임무를 분담하고 해저케이블이 끊어진 상황에 신속하게 대응하기 위해 협력절차를 구체화할 필요가 있다. 이를 통해 해저케이블이 끊어진 상황에 신속하고 효과적으로 대응할 수 있을 것이다. 최근 AUKUS Pillar 2에 한국의 참여가 논의되고 있는데 8개의 협력분야 중 해저전 기술이 포함되어 있다.[57] 해저전 대응역량을 포함한 군사능력을 강화하기 위해 적극적인 참여가 요구된다. 국제 사회

---

53) The White House, "Quad Leaders' Joint Statement," https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-joint-statement/(검색일자: 2024. 2. 2.)

54) Asha Hemrajani, "The QUAD Partnership for Cable Connectivity and Resilience" *RSIS Commentary* No.166(17), NOV. 2023.

55) Hotaka Nakamura, "The Enemy Below: Fighting against Russia's Hybrid Underwater Warfare," Center for Maritime Strategy, 2023. 6.29.

56) Sean Morgan et al., "NATO's Role in Protecting Critical Undersea Infrastructure," CSIS Briefs, 2023.12. pp.4-5.

57) 8개 분야는 해저전, 양자컴퓨터, 극초음속, AI, 사이버, 전자전, 군사혁신, 정보공유 등이다. Rod McGuirk, "South Korea Considers Joining AUKUS Pillar II," *The Diplomat*, 2024. 5. 3.

와의 공동 대응은 해저케이블을 위협하는 잠재적 적성국의 도발 행위를 억제하는 효과로 이어질 수도 있다.

2. 국내적 대응-해저전 대응 거버넌스 구축

해저전은 해군이나 특정 조직 단독으로 대응하기는 불가능하다. 해저전의 특성상 신속하게 알아차리거나 혐의자를 특정하기 어렵다. 공해상 해저에서 발생한 무인체계 간의 전투나 파괴행위의 경우 즉각적으로 대응하기 어려우며 이에 대한 국제법 체계 역시 미비하다.[58] 해저케이블은 길이가 방대하여 전체를 감시하는 것만으로도 많은 시간과 노력이 요구된다. 또한, 해저케이블을 신속히 복구하기 위해서는 다양한 기술과 관계 기관과의 협력이 필요하며, 해저케이블 파괴행위의 용의자가 군이 아닌 민간이거나 적성국의 민간연구소 소속일 경우 해군이 대응하기가 어렵다. 따라서 해저전은 해군뿐만 아니라, 행정안전부, 과학정보통신기술부, 해양수산부, 국정원, 국방부, 해경, 정보통신업체, 케이블 부설 및 유지보수 업체 등이 통합된 거버넌스를 구축하여 대응해야 한다. 최근 이탈리아는 정부와 해군, 민간 부분의 협력을 강화하고 있고 프랑스는 해저전을 정부가 주도하여 국가 전략적 차원에서 부처의 임무를 조율하고 있다. 해저전에 있어 해군의 능력은 여전히 중요하지만, 효과적인 대응을 위해서는 정부 조직을 중심으로 관련 기관과 민간 산업계 간의 적극적 협력체계를 구축하고 임무를 분담해야 한다.

평시 해저전에 대한 대응은 어떤 면에서는 밀수나 해적 대응과 같은 경찰 활동과 다르지 않다. 즉, 정상적인 활동을 하는 수많은 선박 중에서 의심스러운 선박을 식별해야 한다. 이를 위해서는 높은 수준의 해양영역인식(Maritime Domain Awareness)이 필요하다. 해양영역 인식의 핵심은 정보 감시와 공유다. 사실 해양영역인식은 해저전만을 위한 것이 아니라 해양에서 벌어지는 분쟁, 범죄, 해양오염, 경제활동, 항해 안전, 재난 대응 다양한 상황에 대응하는 데 필요하다. 통합된 해양영역인식을 통해 정부, 해군, 해경, 민간의 자산을 사용하여 악의적인 활동을 파악할 수 있다면 감시 및 원인 규명 작업이 상당히 쉬워질 것이다.[59] 국내의 해양감시 역량을 통합하여 우리나라 해저케이블 근처를 저속으로 항해하거나 배회하는 3국 선박을 실시간으로 탐지하고 추적하며, 필요시 선박, 항공기, 무인전력 등을 이용해 근접 확인할 수 있어야 한다. 이는 과학기술의 적용을 통해 더욱 효과적으로 대응할 수 있다. 예를 들어, 선

58) 이기범, "UN 해양법협약은 수중드론(underwater drone) 운용 문제를 규율할 수 있는가?," 『국제법학회논총』, 제62권 제2호, 대한국제법학회, 2017, pp.101-125.

59) Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," *RUSI*, 2023. 5.25.

박의 불규칙한 활동 패턴을 식별하기 위해 빅데이터와 AI 기술을 활용할 수 있다. 통상적으로 움직이지 않는 패턴으로 기동하거나 해저케이블 부설해역 근처를 목적 없이 배회하는 선박 등을 손쉽게 분류해낼 수 있다.

해저케이블에 대한 공격을 받으면 최우선으로 고려해야 할 것은 최단시간내 복구하는 것이다. 해저케이블은 각국 주요 통신사업자들이 컨소시엄을 구성해 유지보수 사업자를 선정한다. 즉, 우리나라 업체가 아닌 미국, 중국, 일본 업체가 선정될 수도 있다. 따라서 고의적인 해저케이블 공격 상황에서 적시적인 대응이 제한될 수 있으며, 전면전이나 국지적인 분쟁이 발생하는 상황에서는 대응 자체가 어려울 수도 있다. 그러므로 우리나라도 미국의 케이블 보안 함대(Cable Security Fleet) 개념을 검토할 필요가 있다. 전시에 대비하여 동원선박을 사전에 지정하고, 유사시 동원할 수 있도록 계약을 맺은 것처럼 해저케이블 유지보수 업체를 지정하고, 계약하여 유사시 즉각적으로 해저케이블 보수작업에 나설 수 있게 하는 것이다. 이를 통해 해저케이블 훼손에 따른 직·간접적인 피해를 최소화할 수 있을 것이다.

3. 군사적 대응-거부적 억제와 보복적 억제

해저전에 대한 군사적 대응은 크게 거부적 억제(deterrence by denial)와 보복적 억제(deterrence by retaliation)로 구분하여 제시한다. 먼저 거부적 억제 방안은 기뢰대항작전(Mine Countermeasure Operation)에서 영감을 얻을 수 있다. 해저전은 본질적으로 절차와 대응 수단 등이 기뢰대항작전과 유사하기 때문이다. 기뢰대항작전이란 적이 부설한 기뢰를 탐색(Hunting)이나 소해(Sweeping)하는 것으로 많은 시간과 노력이 필요하다. 기뢰대항작전은 탐지→접촉→분류→위치결정→확인→처리의 과정을 거치게 되는데,[60] 구역 내 부설된 단 1발의 기뢰 제거에도 많은 시간이 필요하다. 전시 또는 유사시 적이 부설한 기뢰를 보다 신속하게 탐색(Hunting)하기 위해서는 평시에 주요 항만, 해역에 대한 해저 상황을 미리 파악해야 한다. 수중지형, 수중에 있는 구조물, 해저물체 등의 재질이나 위치 정보 등을 미리 파악하고, 유사시나 전시에 탐색한 정보와 차이점을 대조함으로써 보다 신속하게 기뢰대항작전을 수행할 수 있다. 마찬가지로 해저전 대응에 있어 평시 우리나라 해저 인프라에 대한 주기적인 초계나 순찰을 통해 그 정보를 축적해야 하며, 순찰 중 기존에 파악된 정보와 차이점을 발견하면 즉각 정밀히 조사하여 이상 유무를 확인하는 것을 기본으로 대응 방안을 발전시켜야 한다.

---

60) 최현호 "무인기뢰 탐지 및 처리: 해군작전을 위협하는 기뢰 제거를 위한 첨단기술," 『국방과 기술』478호, 한국방위산업진흥회, 2018. pp.60-73.

해저전의 거부적 억제방안은 기뢰대항작전과 유사하나 일부는 다른 면도 있어 이에 대한 고려가 필요하다. 첫째, 작업 공간의 광활함이다. 기뢰대항작전은 주로 항만이나 주요 연안항로에 국한된다. 특히 공격 기뢰는 은밀히 부설해야 하므로 부설 수량에 제한이 있을 수밖에 없다. 따라서 공격 기뢰는 효과를 극대화할 수 있는 항만 근처 항로에 집중되게 된다. 반면 해저전은 해저에 있는 인프라 전체가 공격대상이다. 따라서 기뢰대항작전보다 더 광활한 구역을 대상으로 하며 시간도 더 오래 걸릴 수밖에 없다. 또한, 광활한 해저 공간 전체를 대상으로 하므로 해저 지형에도 큰 영향을 받는다. 특히 높낮이가 심한 해저 경사면의 경우 음탐기(SONAR)를 활용한 탐색 작업이 난반사로 인해 정밀한 식별에 어려움을 겪을 확률이 높다. 따라서 수중카메라를 이용한 식별(Identification)이 요구된다. 다만 해저 인프라는 기뢰보다는 상대적으로 크기가 크며, 연속된 구조물이라는 측면에서 탐색 작업의 이점이 있다. 기뢰대항작전의 경우 수중 암반, 기뢰, 폐기물 등등 다양한 접촉물 등을 일일이 확인해야 하지만, 해저전은 규칙적으로 배열된 구조물 중 불규칙성을 찾아내는 것이라는 점에서 기뢰대항작전보다는 작업이 유리하다.

다음은 보복적 억제를 통한 해저전 대응 방안이다. 우리나라 역시 위협국가의 해저 인프라에 접근할 수 있는 역량을 갖추어 적이 우리 해저 자산을 공격할 시 적 역시 공격받을 수 있음을 인지시켜야 한다. 이를 위해 위협국가의 해저 인프라에 대한 조사와 이에 대한 공격능력을 확보해야 한다. 해저 인프라 조사를 위해서는 수로 조사선과 잠수함을 이용한 심해저 활동역량을 갖추어야 한다. 우리나라는 다른 나라와 달리 핵추진 잠수함을 보유하기가 어려워 재래식 잠수함으로 작전을 해야 하므로 장기간 심해 잠항능력이 제한될 수밖에 없다. 따라서 재래식 잠수함에서 발진하는 무인잠수정을 개발하고 해저 인프라에 대한 작전역량을 갖추어야 한다.

해저전에 투입되는 전력은 유인전력보다는 무인전력이 더 유용하며, 특히 ROV나 AUV 같은 무인잠수정(UUV)을 중점적으로 활용하는 것이 필요하다. 해저 자산의 특성상 해저면에 붙어서 설치되어 있으므로 높은 수압이 작용하는 깊은 심해에서 장기간 머무르며 탐색 작업이 반복적으로 이루어져야 한다. 수상 선박을 이용하면 장비의 유지보수나 기술적 난이도 면에서 이점이 있겠지만 선체 음탐기를 이용한 탐색 작업으로 인해 수중 심도가 깊어질수록 정확도가 떨어지고 카메라 등을 이용한 육안 관찰을 할 수 없다. 또한, 수면상 날씨의 영향도 받기에 지속적인 탐색은 어렵다. 무인잠수정을 이용하면 해저면을 따라 해저 자산의 근거리에서 탐색 작업을 하며 카메라를 이용하여 탐색 작업을 할 수 있으므로 신뢰도가 높다. 더군다나 수면상 날씨의 영향도 받지 않는다. 하지만 깊은 수심에서 장시간 작업하기 위해서는 강한 내압력성과 장기간 작업에 필요한 배터리 기술, 높은 해상도를 가진 합성 개구 소나(Synthetic

Aperture Sonar)[61], 광학장비 등의 장비가 필요하며, 자율주행 성능, 필요시 이상 유무를 판단하고 신속하게 현장 조치나 통제 기지로의 보고를 할 수 있는 AI 성능 등이 필요하다.

Ⅴ. 결론

오늘날 해저케이블과 같은 해저 기반시설들은 마치 발전소, 교량, 도로망 같은 사회기반 시설과 같다. 미래 사회에 미치는 영향을 고려하면 해저케이블은 가장 중요한 기반시설 중 하나다. 지금까지 해양안보가 주로 해상교통로(SLOC)에 중점을 두고 있다면 이제부터는 해저교통망(U-SLOC, Under-sea Lines of Comunication)의 안정성과 효율성을 유지하는 것도 중요하다.[62]

해저전은 무엇이고 왜 중요한가? 해저전이 벌어지는 영역, 그리고 기존의 대잠전과 기뢰전과의 관계에 관한 추가적인 연구와 논의가 필요하지만 본 연구에서 해저전은 "수중 및 해저에서 해저 파이프라인, 해저케이블, 해저 자원 등 해저 자산을 공격하고 보호하기 위해 수행하는 대잠전과 기뢰전을 제외한 모든 작전"으로 정의하였다. 해저전에 대응하는 국제법은 미비하고, 그 특성상 파괴행위를 실시간으로 감시하기도 행위자를 특정하기도 어렵다. 따라서 해저는 하이브리드 전략을 전개하기 적합한 새로운 전장이 되고 있다. 사회 전 분야에 걸쳐 정보통신 네트워크에 의존하는 한국은 해외 인터넷 연결의 99% 이상을 해저케이블에 의존한다. 해저케이블의 수량도 적고, 거제, 부산 등 일부 해역에 몰려있어 해저전의 위협에 취약하다. 비단 북한의 직접적인 위협뿐만 아니라 중국-대만과의 분쟁 상황에서 대만의 해저케이블이 공격을 받으면 한국 역시 피해를 볼 수 있으므로 반드시 이에 대한 대응방안을 마련해야 한다.

주요 국가들은 해저전을 어떻게 준비하고 있는가? 세계 주요 국가들은 해저전을 심각하게 받아들이고 있고 이에 대해 준비하고 있다. 중국과 러시아는 최고수준의 해저전 공격능력을 가진 것으로 평가되고 있다. 미국, 프랑스, 영국과 같은 민주진영 국가들은 해저전 대응을 위한 개념을 연구하고 관련 전력을 도입하고 국제 및 국내 협의체를 구성하는 등 발 빠르게 움직이고 있다. 최근 노르트스트림 폭발, 발트해와 홍해에서 해저케이블 손상은 해저전이 이제 실존하는 위협임을 무겁게 인식하는 계기

61) 송수신 센서를 이동하면서 같은 해저면에 다수의 소나핑을 투사하여 여러 위치에서 취득한 데이터를 합쳐 기존 사이드스캔소나(Side Scan SONAR)보다 10배 높은 해저면을 탐색할 수 있는 음탐기, 이지은 외, "예인형 합성개구 소나 시스템(SAS) 개발," 『Journal of the KNST』, Vol.2, No.1, 한국해군과학기술학회, 2019. p.28.

62) 임경한, "해군의 시각에서 보는 신기술·사이버안보 이슈," 이슈브리핑 No.178, 서울대학교 국제문제연구소, 2024. 4.18.

가 되었다.

해저전에 대응하기 위해 무엇을 해야 하는가? 공해상에 여러 나라와 연결되어 설치된 해저케이블 특성상 주변국과의 협력이 필수적인데 특히, 규칙기반의 해양질서를 공유하는 미국, 일본, 대만, 호주와의 소다자주의에 의한 대응이 필요하다. 국내에서는 정부 기관, 해군, 해경, 관련 업체와의 거버넌스를 구축하여 통합적인 대응이 요구된다. 특히 손상된 케이블을 신속히 복구하기 위해 케이블 보안 함대 제도를 도입할 필요가 있다. 군사적 대응으로는 기뢰대항작전과 유사하게 평소 해저케이블을 현황을 주기적으로 조사하고 이상 유무를 확인하고 대응하는 거부적 억제와 유사시 위협국가의 해저 인프라에 접근할 수 있는 보복적 억제 능력을 동시에 보유해야 한다.

참 고 문 헌

1. 저서

한국지능정보사회진흥원, 『2022 한국인터넷 백서』, 대구: 한국지능정보사회원, 2023.

JCS, *Joint Maritime Ops,* Washington DC: Joint Chief of Staff, 2023.

Ministère des Armées, *French Seabed Warfare,* Paris: Ministère des Armées, 2022.

2. 논문

고명현·임정희, "해저케이블망과 데이터 안보," 이슈브리프 2022-35호, 아산정책연구원, 2022.12.29.

고성협 외, "만타형 무인 잠수정의 개발과 실해역 성능시험," Journal of the Korean Society of Marine Engineering, Vol.37, No.6, 한국마린엔지니어링학회, 2013.

김채형, "해저케이블 부설과 이용에 관한 국제사회의 법적 체제," 『해사법연구』제29권 제1호, 한국해사법학회, 2017.

심세현, "디지털 기술의 발전과 사이버안보 위협," 『국가와 정치』제29집 1호, 동아시아연구소, 2023.

오일석, "해저케이블을 통해 전송되는 정보와 데이터의 안정성 확보 방안," 이슈브리프 330호, 국가안보전략연구원, 2022.

온대원, "하이브리드 안보위협에 대한 EU의 대응정책," 『EU연구』제59호, 한국외국어대학교 EU연구소, 2021.

유준구, "사이버작전 시 유엔해양법 원칙 적용의 현안과 과제," 『IFANS 주요국제문제 분석』, 2022-45호, 국립외교원 외교안보연구소, 2022.

이기범, "UN 해양법협약은 수중드론(underwater drone) 운용 문제를 규율할 수 있는가?," 『국제법학회논총』, 제62권 제2호, 대한국제법학회, 2017.

이지은 외, "예인형 합성 개구 소나 시스템(SAS) 개발," 『Journal of the KNST』, Vol.2, No.1, 한국해군과학기술학회, 2019.

임경한, "해군의 시각에서 보는 신기술·사이버안보 이슈," 이슈브리핑 No.178, 서울대학교 국제문제연구소, 2024. 4.18.

최현호, "해저 인프라 보호 강조되는 해저전: 기뢰전에서 해저케이블 보호까지 확대되는 해저 작전," 『국방과 기술』539호, 한국방위산업진흥회, 2024.

_____, "무인기뢰 탐지 및 처리: 해군작전을 위협하는 기뢰 제거를 위한 첨단기술," 『국방과 기술』478호, 한국방위산업진흥회, 2018.

Burnett, Douglas R., "Submarine Cable Security and International Law," *International Law Studies*, Vol.97, 2021.

_____, "Repairing Submarine Cables Is a Wartime Necessity," *Proceedings*, Vol.148/10/1,436, 2022.10.

Davenport, Tara, “Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis,” Cath. U. J. L. & Tech Vol.24, 2015.

Hemrajani, Asha, “The QUAD Partnership for Cable Connectivity and Resilience” *RSIS Commentary* No.166(17), NOV. 2023.

Morgan, Sean et al., “NATO’s Role in Protecting Critical Undersea Infrastructure,” *CSIS Briefs*, 2023.12.

3. 기타자료

김범수, “베트남, 인터넷 개선되나…‘고장’ 해저케이블 5개 중 1개 수리, 연합뉴스, 2023. 4.28.

변휘, “‘초연결 세계’ 무너뜨린 해저화산…한국인터넷은 안전할까,” 머니투데이, 2022. 1.22.

차종환, “국경 없는 데이터 고속도로, ‘해저케이블’ 관심집중,” 정보통신신문, 2023. 9.22.

최일, “해저전,” SPNNews, 2023.10.30.

한지연, “LS마린솔루션, 아태 해저케이블 유지보수 맡는다…年130억 수익,” 머니투데이, 2023. 9. 8.

Ahlander, Johan, “Sweden ends Nord Stream sabotage probe, hands evidence to Germany,” *REUTERS*, 2024. 2. 8.

Batra, Nishant, “Technology Strategy 2030: Nokia’s guide to the emerging technologies that are radically changing our world,” NOKIA, 2023. 11. 8. https://www.nokia.com/about-us/newsroom/articles/introducing-nokias-technology-strategy-2030/(검색일자: 2024. 1.10.)

Berglund, Nina, “Surveillance cables mysteriously cut,” *NEWSinENGLISH*, 2017. 11. 7.

Brooke-Holland, Louisa, “Seabed warfare: Protecting the UK’s undersea infrastructure,” *House of Commons Library*, 2023. 5.24.

CPNI, “An Overview of the Use of Submarine Cable Technology by UK PLC,” https://cyberwar.nl/d/20060300_Submarine-cables_CPNI-UK.pdf(검색일자: 2024. 2.21.)

Glenney, Bill, “The Deep Ocean: Seabed Warfare And The Defense Of Undersea Infrastructure, Pt. 1,” *CIMSEC*, 2019. 2. 4.

House of Commons, “We’re going to need a bigger Navy,” https://committees.parliament.uk/committee/24/defence-committee/news/159793/were-going-to-need-a-bigger-navy/(검색일자: 2024. 2.21.)

Insightunboxed, “Technology Proliferation: Threat or Opportunity?,” *Insightunboxed*, 2019. 5.14.

Kaushal, Sidharth, “Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure,” *RUSI*, 2023. 5.25.

Lee, Christy, "North Korean Missiles Used by Russia Against Ukraine Are Products of Sanction Loopholes," *VOA*, 2024. 2.27.

Rod McGuirk, "South Korea Considers Joining AUKUS Pillar II," *The Diplomat*, 2024. 5. 3.

Mims, Christopher, "Google, Amazon, Meta and Microsoft Weave a Fiber-Optic Web of Power," *The Wall Street Journal*, 2022. 1.15.

Nakamura, Hotaka, "The Enemy Below: Fighting against Russia's Hybrid Underwater Warfare," *Center for Maritime Strategy*, 2023. 6.29.

NOKIA, Global Network Traffic 2030 Report, 2023.(https://onestore.nokia.com) asset/213660(검색일자: 2024. 1.10)

Panneerselvam, Prakash, "Unmanned Systems in China's Maritime 'Gray Zone Operations'," *The Diplomat*, 2023. 1.23.

Salerno-Garthwaite, Andrew, "Seabed warfare is a 'real and present threat'," *Naval Technology*, 2022.12.20.

Suciu, Peter, "USS Jimmy Carter: The Navy Has a Spy Submarine That Can't Be Matched," *The National Interest*, 2023.11.23.

Sutton, H. I. "Russia's Growing Secret Submarine Fleet Key to Moscow's Undersea Future," *USNI News*, 2021.11.30.

_____, "U.S. Navy To Get New Unique Submarine: Virginia SSW," *Naval News*, 2023. 4.20.

Telegeography, The State of the Network, 2023. https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2023.pdf(검색일자: 2024. 1.10.).

The White House, "Quad Leaders' Joint Statement," https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-joint-statement/(검색일자: 2024. 2. 2.).

Upadhayaya, Venus, "Seabed Warfare is New Domain in CCP's Quest to Dominate the Indo-Pacific," *The EPOCH TIMES*, 2023.10.13.

Vigliarolo, Brandon, "Underwater cables in Red Sea damaged months after Houthis threatened to do just that," *The Register*, 2024. 2.27.

Wendorf, Marcia, "Operation Ivy Bells: The U.S. Top-Secret Program That Wiretapped a Soviet Undersea Cable," *Interesting Engineering*, 2022. 1. 3.

Werner, Ben, "Billionaire Paul Allen Finds Lost World War II Cruiser USS Indianapolis in the Philippine Sea," *USNI News*, 2017. 8.19.

https://oceanexplorer.noaa.gov/facts/deep-ocean.html(검색일자: 2024. 1.15.)

http://www.hisutton.com/Spy%20Sub%20-%20Project%2010831%20Losharik.html(검색일자: 2024. 2.15.).

https://www.iscpc.org/(검색일자: 2024. 1.15.).
https://www.submarinecablemap.com/(검색일자: 2024. 1.15.).
中国国务院, “十三五国家科技创新规划的通知,” https://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm(검색일: 2024. 2.23.).

Abstract

A Study on Countermeasures on Seabed Warfare: Focused on Submarine Cables

Cho, Seong-jin, Lim, Soohoon
(ROK Naval Future Innovation Research Group)

The Nord Stream explosion and the damage to submarine cables in the Baltic Sea and Red Sea have raised interest in seabed warfare all the world. And each country is preparing response plans and strategy. However, although South Korea relies on submarine cables for most of its internet network and is vulnerable to threats from North Korea and neighboring countries, even the term Seabed Warfare is unfamiliar. This paper is the first domestic study to analyze the definition and characteristics of seabed warfare, the current status of each country, and suggest countermeasures. In order to respond to seabed warfare, I propose establishing a cooperative system based on Mini-multilateralism between countries that share an international rules-based order, and establishing governance with related domestic organizations and companies. And I propose a military response plan based on deterrence by denial and deterrence by retaliation

Key Words: Seabed Warfare, Subsea Warfare, submarine cable, Seabed Infrastructure, Countermeasures on Seabed Warfare

투고일: 2024년 2월 29일 | **심사일:** 2024년 4월 14일 | **심사완료일:** 2024년 5월 17일