기본연구 2025-05

해양 복합위협의 실효적 대응 방안 연구

A Study on Effective Countermeasures against Maritime Hybrid Threats

민영훈 · 윤인주 · 임병호 · 황수연 · 조익순



KMI 한국해양수산개발원
KOREA MARITIME INSTITUTE

기본연구 2025-05

해양 복합위협의 실효적 대응 방안 연구

A Study on Effective Countermeasures against Maritime Hybrid Threats

민영훈 · 윤인주 · 임병호 · 황수연 · 조익순

KMI 한국해양수산개발원
KOREA MARITIME INSTITUTE

저자	**민영훈, 윤인주, 임병호, 황수연, 조익순**
내부연구진	연구책임자 민영훈 한국해양수산개발원 글로벌전략연구본부 전문연구원 공동연구원 윤인주 한국해양수산개발원 글로벌전략연구본부 연구위원 공동연구원 임병호 한국해양수산개발원 글로벌전략연구본부 부연구위원 공동연구원 황수연 한국해양수산개발원 해양연구본부 전문연구원
외부연구진	공동연구원 조익순 국립한국해양대학교 교수

연구기간	2025. 1. 1. ~ 2025. 10. 31.

보고서 집필내역

연구책임자	민영훈 연구총괄, 제1장, 제2장 제1절-제2절 제4절 일부, 제4장 제1절 제3절 제4절, 제5장, 제6장
내부연구진	윤인주 제3장 임병호 제4장 제2절 일부 황수연 제2장 제3절, 제4절 일부
외부연구진	조익순 제4장 제2절 일부

산·학·연·정 연구자문위원	류춘열 인천항보안공사 사장 이도엽 부산항만공사 과장 이상일 국립한국해양대학교 교수 이호근 해양수산부 항만안전보안과 사무관 윤기성 해양경찰청 경정

※ 순서는 산·학·연·정 순임

발간사

해양을 둘러싼 국제 환경은 최근 그 어느 때보다 빠르고 복잡하게 변화하고 있다. 기후위기의 가속화로 인한 해양 생태계의 구조적 변화, 국가 간 해양영토 및 해양자원 경쟁의 심화, 사이버·기술 기반의 새로운 형태의 비전통 안보 위협의 등장, 글로벌 해운·물류망의 불안정성, 자연재해와 인적 요인이 복합적으로 결합하여 나타나는 재난의 증가 등은 모두 해양공간이 직면한 새로운 도전이며, 이러한 요소들은 단순히 개별적으로 존재하는 것이 아니라 상호 연계되고 중첩되어 '해양 복합위협'이라는 형태로 나타나고 있다. 우리나라는 해양을 국가경제의 핵심축으로 삼아 성장해온 만큼, 이러한 변화가 가져오는 영향은 매우 직접적이며, 해양 복합위협을 선제적으로 진단하고 대비하는 것은 국가적 차원의 중요한 과제가 되었다.

한국해양수산개발원(KMI)은 이러한 문제의식을 바탕으로 "해양 복합위협의 실효적 대응 방안 연구"를 기본과제로 수행하였다. 이번 연구는 해양 복합위협이라는 개념 자체가 아직 국내에서 충분히 정립되지 않은 상황에서, 해양 복합위협의 개념을 다층적인 관점에서 정리하고, 우리나라 해양환경에 특화된 위협의 실체를 밝히며, 궁극적으로 국가적 대응 체계를 마련하기 위한 정책적 기반을 구축하는 데 목적이 있다. 해양 복합위협은 자연적, 인적, 기술적, 사회경제적 요인이 서로 얽혀 나타나는 특징이 있음에도 불구하고, 기존의 대응체계는 주로 개별 분야 중심으로 작동해 왔다. 더욱이 해양에서 발생하거나 해양과 관련된 복합위협의 경우, 초기 대응, 단속, 조사, 사후 처리 등과 관련하여 다양한 기관이 개입될 수 있어, 이를 효과적으로 관리하고 조정하기 위한 정책 또는 제도가 필요하다. 따라서 본 연구는 해양 주권을 수호하고 우리 바다를 국민이 안전하게 활용하게 하기 위해 해양 복합위협을 예방부터 대응까지 효과적으로 대응하기 위한 정책적 방안을 제안했다.

먼저, 본 연구는 연구의 대상과 범위를 명확하게 하기 위해 해양 복합위협의 개념을 체계적으로 정립한다. 이를 위해 해양 복합위협은 단순히 여러 위험이 존재하는 것이 아니라, 서로 다른 영역의 위협이 시간적·공간적으로 중첩되며 예측과 대응을 어렵게 하는 특징이 있다는 점을 다양한 연구를 통해 확인했다. 또한 본 연구에서는 국내외 다양한 해양 복합위협 사례를 검토하여 실제 피해 사례와 위험 확산 구조를 분석하였으며, 이를 통해 모든 해양 복합위협을 개별 기관의 제한된 국가 자산으로 감시하고 대응하는 것이 어렵다는 것을 확인했다. 예를 들어, 자율운항선박을 온라인 해킹을 통

해 탈취하고, 탈취한 선박을 발전소 등 해양 주요시설을 공격하는데 활용하거나 불법 화물을 환적하거나 이송하여 또 다른 위협으로 연계하는 경우, 행위자의 위치 확인, 발생 위협의 대응 등과 관련하여 경찰청, 해양경찰청, 관세청, 출입국외국인청, 국가사이버안보센터 등이 개입될 수 있다. 그리고 항만물류시스템에 대한 사이버 위협 등은 국가 기간 공급망을 혼란스럽게 하거나, 항만 안전을 동시에 위협할 수 있고 이러한 위협을 대응하기 위해서는 정책적으로 해양수산부, 정책이행과 관련해서는 해양경찰청 등이 개입될 수 있다. 이러한 복합적 구조는 기존의 개별 분야 중심의 대응 체계가 협력적으로 원활히 작동될 때 효과성을 기대할 수 있다. 이에 본 연구는 해양 복합위협 대응 관련 국내·외 대응 체계 또한 분석 및 비교하여, 현재 국내 대응 체계가 개별 기관의 역할과 협력에 의존하여 운용되고 있음을 확인하고 이는 해양 복합위협의 예방 및 대비에 다소 한계가 있음을 확인할 수 있었다.

한편 본 연구는 우리나라의 해양 복합위협 대응체계를 제도적·조직적·운영적 측면에서 진단하였다. 중앙정부와 지방정부, 다양한 공공기관, 관련 산업계 등 여러 주체가 각각의 역할을 수행하고 있으나, 해양 복합위협 관점에서 여전히 정책의 분절성이 존재하고, 기관 간 정보 공유 체계가 충분히 구축되지 못한 점이 확인되었다. 특히 위기대응 과정에서 기관 간 협조 체계가 일시적이고 상황 의존적으로 작동하는 경우가 많아, 상시적이고 통합적인 대응체계 구축의 필요성이 강조되었다. 또한 해양 복합위협의 특성상 데이터의 공유와 통합이 매우 중요함에도 불구하고, 현재의 정보 인프라는 개별 기관 중심으로 운영되고 있어, 다원적 정보를 결합한 위험 예측이나 종합적 의사결정 지원에는 한계가 있는 것으로 나타났다. 이에 본 연구는 기술적·시스템적 접근을 통해 대응 역량을 강화할 필요성을 제기하였다. 위험 기반의 해양 위험 관리 모델, 다원적 데이터 통합 플랫폼 등이 해양 복합위협 대응의 핵심적 요소로 검토되었다. 기술적 기반은 단기적인 대응뿐 아니라 장기적인 전략 수립에도 필수적이며, 특히 위기 발생의 사전 예측과 신속한 대응을 위해서는 데이터 기반의 '상황 인지 능력'을 강화하는 것이 중요하다는 점이 강조되었다.

이 연구에서 가장 중요한 부분 중 하나는 국가적 대응전략과 정책과제를 종합적으로 제시한 것이다. 본 연구는 해양 복합위협 대응을 위해 국가 차원의 통합형 대응체계를 구축하는 것이 무엇보다 중요하다고 강조하였다. 이를 위해 부처 간 정책을 연결하는 거버넌스 체계를 구축하고, 지자체와 민간기업, 산업계가 참여하는 연계형 협력

체계를 마련해야 하며, 국제 협력의 확대 또한 필수적이다. 해양 복합위협은 특정 국가의 문제로 국한되지 않기 때문에, 국제기구와 주변 해역 국가들과의 협력을 강화하고 공동 대응 체계를 마련하는 것이 장기적으로 매우 중요한 과제임이 확인되었다.

한국해양수산개발원은 이번 연구를 통해 해양 복합위협이라는 새로운 정책 환경을 보다 체계적으로 이해하고, 국가적 대응 전략 수립에 필요한 기초 자료를 제공하고자 하였다. 해양 복합위협은 단일 기관이나 특정 분야가 단독으로 해결할 수 있는 문제가 아니며, 다양한 이해관계자 간의 협력과 과학적 분석에 기반한 정책적 접근이 요구되는 문제이다. 본 연구가 우리나라의 해양정책 전반에 걸쳐 중요한 시사점을 제공하고, 해양안전과 해양안보, 지속가능한 해양 이용과 산업 발전을 위한 정책 수립에 실질적인 도움이 될 수 있기를 기대한다. 특히 해양 복합위협에 대한 이해는 앞으로 우리나라의 해양 전략 수립뿐 아니라, 국제적 협력과 글로벌 해양 거버넌스에 참여하는 데에도 중요한 기반이 될 것으로 생각된다.

끝으로 어려운 여건 속에서도 연구를 성실히 수행해 준 연구진과 관련 전문가 여러분께 깊은 감사의 말씀을 드린다. 특히, 해양 복합위협이라는 다소 생소한 주제를 분석하기 위해 주도적으로 연구를 이끌어온 민영훈 전문연구원을 비롯하여, 윤인주 연구위원, 황수연 전문연구원, 임병호 부연구위원에게 깊은 감사를 표한다. 또한 현장의 자문과 조언을 아끼지 않으신 여러 전문가와 관계기관에도 감사를 드린다. 연구의 질과 성과 향상을 위해 자문과 인터뷰로 도움을 주신 해양경찰청 윤기성 경정, 해양 국제범죄 통계 및 GIS 분석을 수행하신 국립한국해양대학교 조익순 교수, 그리고 대응 방안과 정책 제언에 대해 자문해 주신 해양경찰청 서상욱 경정과 관련 전문가에게 특히 감사의 뜻을 전한다. 산·학·연·정 관계자 및 전문가들의 자문과 도움이 없었다면 이 연구는 불가능했을 것이다.

한국해양수산개발원은 앞으로도 해양수산 분야의 미래 전략을 이끌어 나가는 국가적 싱크탱크로서, 국민의 안전과 국가의 지속가능한 발전을 위해 연구 역량을 더욱 강화하고 책임 있는 역할을 다할 것이다.

2025년 12월
한국해양수산개발원
원장 조 정 희

목차

정책제안 _ i

요약 _ iii

Executive Summary _ xiii

01 서론 _1

제1절 연구 필요성 및 목적 1
1. 연구 배경 및 필요성 1
2. 연구 목적 9

제2절 연구 범위 및 방법 11
1. 연구 범위 및 주요 내용 11
2. 연구 방법 15

제3절 선행연구 검토 18
1. 선행연구 분석 18
2. 선행연구와의 차별성 19

02 해양 복합위협의 이론적 검토 및 주요 사례 분석 _23

제1절 해양 복합위협 국내외 논의 동향 23
1. 해양 복합위협 국외 논의 동향 23
2. 해양 복합위협 국내 논의 동향 27

제2절 해양 복합위협의 정의 및 범위 33
1. 해양 복합위협의 개념과 정의 33
2. 해양 복합위협의 범위와 유형 36

제3절 해양 복합위협 주요 사례 분석 46
1. 해양 국제범죄 주요 사례 분석 46
2. 해양테러 및 해양 사이버위협 주요 사례 분석 63

제4절 실효적 대응방안 필요성 80

03 해양 복합위협 대응체계 국외 사례 분석 _85

제1절 미국의 해양 복합위협 대상과 대응체계 86
1. 관리 대상 및 범위 86
2. 관리제도 및 대응체계 88

제2절 일본의 해양 복합위협 대상과 대응체계 97
1. 관리 대상 및 범위 97
2. 관리제도 및 대응체계 99

제3절 영국의 해양 복합위협 대상과 대응체계 104
1. 관리 대상 및 범위 104
2. 관리제도 및 대응체계 106

제4절 국제 비교 분석 및 국내 적용 시사점 112
1. 국가별 특징 및 대응체계 비교 112
2. 실효적 대응방안 시사점 117

04 해양 복합위협 국내 대응체계와 데이터 분석 _121

제1절 해양 복합위협 국내 대응체계 121
1. 해양 국제범죄 국내 대응체계 122
2. 해양테러 국내 대응체계 138
3. 해양 사이버위협 국내 대응체계 141

제2절 해양 복합위협 발생 현황 및 GIS 분석 148
1. 해양 복합위협 발생 현황 분석 148
2. 해양 복합위협 GIS 분석 161

제3절 해양 복합위협 위험성 분석 176
1. 해양위협 위험성 평가 모델(MSRAM) 177
2. 해양위협 위험성 평가 결과 181

제4절 국내 대응체계 한계 및 데이터 분석 시사점 189
1. 분절적 대응체계 및 책임의 모호성 189
2. 데이터 분석에 따른 정책 우선순위 192

05 해양 복합위협의 실효적 대응 방안 _195

제1절 해양 복합위협의 실효적 대응을 위한 정책 방향 195
제2절 해양 복합위협의 효과적 대응을 위한 정책 방안 200
1. 해양 복합위협 통합 대응체계 구축 200
2. 해양 복합위협 대응 국가전략 수립 216
3. 해양 복합위협 위험성 평가 제도 도입 220
제3절 정책 방안의 기대효과 227
1. 정책·경제적 기대효과 227
2. 사회·기술적 기대효과 228

06 결론 및 정책 제언 _231

제1절 요약 및 결론 231
제2절 정책 제언 241
1. 통합적 거버넌스 및 국가전략의 제도화 241
2. 해양 복합위협 위험성 평가 및 정보분석플랫폼 구축 243
제3절 후속과제 245
1. 해양 복합위협 관련 정보 수집 및 관리 체계 구축 연구 245
2. 해양 복합위협 위험성 평가 모델 개발 연구 246

참고문헌 _249

부록 _269

표 목차

〈표 1-1〉 국내 주요 해상 마약 단속 사례 ····· 3
〈표 1-2〉 최근 주요 밀입(출)국 시도 사례 ····· 5
〈표 1-3〉 주요 해양 국제범죄 발생 현황(최근 5년) ····· 6
〈표 1-4〉 정책협의회 및 전문가 자문 등 ····· 17
〈표 1-5〉 선행연구와의 차별성 ····· 20
〈표 2-1〉 복합위협과 해양 복합위협 정의 ····· 35
〈표 2-2〉 사이버위협의 종류 ····· 40
〈표 2-3〉 사이버 범죄의 유형 ····· 40
〈표 2-4〉 사이버 테러리즘의 유형 ····· 41
〈표 2-5〉 해양 복합위협의 범위 ····· 42
〈표 2-6〉 국외 해양 복합위협의 유형 ····· 43
〈표 2-7〉 해양 복합위협의 유형 및 행위 ····· 45
〈표 2-8〉 밀입(출)국 사례 분석 요약 ····· 53
〈표 2-9〉 마약 등 밀수(매) 및 불법 화물 해상운송 사례 분석 요약 ····· 61
〈표 2-10〉 한-중 해저케이블 절단 사고의 기관별 대응 및 후속 처리 ····· 64
〈표 2-11〉 예멘 후티 무장세력 무인수상정의 미국 화물 선적 상선 공격 사례의 기관별 대응 및 후속 처리 ····· 70
〈표 2-12〉 미국 시애틀 항만청 사이버 공격 사례의 기관별 대응 및 후속 처리 ····· 72
〈표 2-13〉 일본 나고야 항만청 랜섬웨어 공격 사례의 기관별 대응 및 후속 처리 ····· 75
〈표 2-14〉 실효적 대응방안 필요성 도출 ····· 83
〈표 3-1〉 미국 국토안보부의 안보와 위협 분류 ····· 86
〈표 3-2〉 해양에서 발생하는 위협의 대표 유형 ····· 87
〈표 3-3〉 해양 복합위협 관련 미국 연방 법률 ····· 91
〈표 3-4〉 일본의 해양기본계획과 방위백서에 나타난 위협 분류 ····· 98
〈표 3-5〉 영국 교통부의 해양위협 분류 ····· 105
〈표 3-6〉 미국·일본·영국의 해양 복합위협 대응체계 요약 ····· 114
〈표 3-7〉 국가별 해양 복합위협 1차 대응 기관 권한 비교 ····· 116
〈표 3-8〉 국가별 해양 복합위협 대응체계 ····· 116
〈표 4-1〉 해양 국제범죄 유형, 범죄 종류 및 근거 법령 ····· 122
〈표 4-2〉 해양 국제범죄 유형별 대응 기관(밀입(출)국, 밀수(출)입) ····· 125

〈표 4-3〉 밀입(출)국 및 밀수(출)입 관련 해양 국제범죄 발생 현황 ····· 127
〈표 4-4〉 해양 국제범죄 유형별 대응 기관 ····· 131
〈표 4-5〉 항만법 제2조 제5호의 항만시설 ····· 136
〈표 4-6〉 해양테러 유형 및 행위 ····· 138
〈표 4-7〉 대테러활동 개념 ····· 141
〈표 4-8〉 해양 사이버범죄 유형 ····· 144
〈표 4-9〉 연도별 국제범죄 발생 건수 현황 ····· 149
〈표 4-10〉 범죄 유형별 발생 건수 통계분석(2020년~2024년) ····· 151
〈표 4-11〉 계절별 발생 건수 분석(2020년~2024년) ····· 152
〈표 4-12〉 범죄 분야별 관계기관 배정 ····· 161
〈표 4-13〉 범죄 유형별 발생 건수와 해상교통량 상위 20% 중첩 비율 ····· 175
〈표 4-14〉 범죄 유형별 발생 건수와 해상교통량 상위 20% 미중첩 비율 ····· 176
〈표 4-15〉 해양 복합위협 유형, MSRAM 공격 수단, 해양 국제범죄 유형 ····· 179
〈표 4-16〉 해양 복합위협 위험성 순위 ····· 182
〈표 4-17〉 해양 복합위협 발생가능성 순위 ····· 183
〈표 4-18〉 해양 복합위협 취약성 순위 ····· 185
〈표 4-19〉 해양 복합위협 영향 순위 ····· 186
〈표 5-1〉 해양 복합위협 공간별 책임 분산 구조 ····· 203
〈표 5-2〉 관련기관 해양 복합위협 대상별 책임 분산 구조 ····· 205
〈표 5-3〉 협의체별 해양 복합위협 대상별 책임 분산 구조 ····· 207
〈표 5-4〉 「해양 (복합)위협 관리법」(가칭) 주요 내용 ····· 215
〈표 5-5〉 MSRAM 평가 요소 ····· 223
〈표 5-6〉 위험성 평가 결과 활용 방안 ····· 224
〈표 5-7〉 해양 복합위협 위험성 평가 지침 주요 구성 ····· 225
〈표 5-8〉 정책 방안의 기대효과 ····· 229

그림 목차

〈그림 1-1〉 해양경찰청 마약사범 단속 현황(2015년~2024년) ····· 2
〈그림 1-2〉 연도별 마약사범 단속 현황(2012년~2023년) ····· 4
〈그림 1-3〉 연도별 해양시설 사이버 침해 현황 ····· 7
〈그림 1-4〉 본 연구의 목적과 정부 국정과제 연관성 ····· 11
〈그림 1-5〉 연구 추진체계 ····· 15
〈그림 3-1〉 미국 GMCC와 MORT체계 ····· 96
〈그림 4-1〉 마약류대책협의회 기능 및 기관별 역할 ····· 124
〈그림 4-2〉 관세청 연도별 마약사범 단속 현황(2020년~2024년) ····· 126
〈그림 4-3〉 해역별 해적위험지수 현황 ····· 130
〈그림 4-4〉 해양 국제범죄 대응체계 ····· 133
〈그림 4-5〉「국제선박항만보안법」에 따른 대응체계 ····· 137
〈그림 4-6〉「테러방지법」상 테러 대응체계 ····· 140
〈그림 4-7〉「해사 사이버안전 관리지침」상 해사 사이버안전 보안 체계 ····· 143
〈그림 4-8〉 선박입항 통계(2024~2025) ····· 145
〈그림 4-9〉 국가사이버안보 수행체계 ····· 147
〈그림 4-10〉 국제범죄 발생 건수(2020년~2024년) ····· 150
〈그림 4-11〉 계절별 해양 국제범죄 발생 현황 ····· 153
〈그림 4-12〉 월별 출입국문란 범죄 현황 ····· 154
〈그림 4-13〉 월별 밀수입·수출 범죄 현황 ····· 154
〈그림 4-14〉 월별 마약류관리법 범죄 현황 ····· 155
〈그림 4-15〉 월별 해양환경관리법 범죄 현황 ····· 156
〈그림 4-16〉 시간대별 범죄 발생 현황 ····· 158
〈그림 4-17〉 연도별 평균 발생 현황과 변동성 ····· 159
〈그림 4-18〉 연도별 발생 현황, 증가율, 변동성 분석 결과 ····· 160
〈그림 4-19〉 범죄 발생 위치, 시군구별 범죄 발생 횟수 ····· 162
〈그림 4-20〉 국제범죄 관계기관 위치, 시군구별 기관 개수 ····· 163
〈그림 4-21〉 해양 국제범죄 분포 위치 ····· 164
〈그림 4-22〉 해양 국제범죄 핫스팟 분석 결과 ····· 165
〈그림 4-23〉 해양 국제범죄 계절별 핫스팟 분석 결과 ····· 166
〈그림 4-24〉 시간대별 핫스팟 분석 결과(00시~12시) ····· 167

〈그림 4-25〉 시간대별 핫스팟 분석 결과(12시~24시) ····· 168
〈그림 4-26〉 기관별 해양 국제범죄 핫스팟 분석 결과(1) ····· 169
〈그림 4-27〉 기관별 해양 국제범죄 핫스팟 분석 결과(2) ····· 170
〈그림 4-28〉 기관별 핫스팟 분석 기반 취약 해역 및 지역 분석 결과(1) ····· 172
〈그림 4-29〉 기관별 핫스팟 분석 기반 취약 해역 및 지역 분석 결과(2) ····· 173
〈그림 4-30〉 우리나라 연안 해상교통량 분석 결과 ····· 174
〈그림 4-31〉 USCG MSRAM 평가 모델 ····· 178
〈그림 4-32〉 해양 복합위협 위험성 평가 모델 ····· 181
〈그림 4-33〉 USCG MSRAM 위험성 분석 모델 및 정책 대응 방향 ····· 187
〈그림 4-34〉 해양 복합위협 위험성 분석 ····· 188
〈그림 5-1〉 해양 복합위협 통합적 대응체계 ····· 197
〈그림 5-2〉 해양 복합위협 실효적 대응 방안 방향 ····· 200
〈그림 5-3〉 국가해양위협대책위원회(가칭) 운영 체계 ····· 210
〈그림 5-4〉 USCG MSRAM 위험성 평가 결과 예시 ····· 212
〈그림 5-5〉 국가해양위협대책위원회(가칭) 구축 로드맵 ····· 214
〈그림 5-6〉 해양 복합위협 대응 국가전략 개념도 ····· 219

정책제안

▌분석 내용 및 방법

1. 본 연구는 복합적이고 다면적인 특성을 가진 연구 대상인 해양 복합위협을 분석하기 위해 정성적 분석과 정량적 분석을 교차적으로 활용.

2. 정성적 분석의 경우, 해양 복합위협 주요 사례와 주요국 해양 복합위협 대응 제도 및 체계와 국내 대응체계를 비교 분석하였음. 해양 복합위협 주요 사례 분석을 통해 최근 해양 복합위협의 발생 원인, 수단, 영향 등을 확인할 수 있었으며, 미국, 일본, 영국 등 주요국의 복합위협 대응 제도, 체계 등을 분석하여 국내 대응체계와 달리 다양한 기관과 국가 자원이 효율적으로 운용될 수 있는 거버넌스를 구축하고 있음을 확인할 수 있었음

3. 정량적 분석의 경우, 해양 국제범죄 발생 통계, GIS 정보, 해양 복합위협의 전문가 설문을 통한 위험성 평가를 실시. 이를 통해, 전통 해양 복합위협인 해양 국제범죄의 발생 경향과 대응 우선 순위 및 방향 등을 분석할 수 있었음. 해양 국제범죄 GIS 정보 분석을 통해 관련 부처 단속과 해양 국제범죄 발생 위치 간의 관계를 간접적으로 확인하였으며, 또한 해양 복합위협 위험성 평가를 통해 신흥 위협의 우선 순위를 확인할 수 있었음

▌정책제안

1. 본 연구는 분석을 통해 우리나라 현재 체계가 해양 복합위협을 실효적으로 대응하기에 다소 미흡한 것으로 확인하고, 특히, 발생 현안 별로 관련 기관의 분절적 대응이 관할의 중첩으로 이어지거나, 감시의 사각으로 연결될 수 있음을 확인했음

2. 또한, 해양 복합위협의 비정형화, 국제화, 대형화, 전문화되는 것을 고려할 때, 위협의 예방 및 대비가 중요해짐에도 불구하고 마약 단속, 대테러 등 특정 분야의 협력체계를 제외하고 관련 기관간 포괄적 협력체계를 확인하기 어려워, 예방, 대비, 대응, 복구 등 전 주기에 걸친 실효적 대응 체계 수립이 필요한 것을 확인함

3. 본 연구는 정책제언으로 통합적 거버넌스 및 국가전략의 제도화와, 해양 복합위협 위험성 평가 및 정보분석플랫폼 구축을 제시함.

4. 통합적 거버넌스 및 국가전략의 제도화는 해양 복합위협을 실효적으로 대응하기 위한 통합적 거버넌스를 제도적으로 구축하고 이를 이행하기 위한 국가 전략을 수립하여 지속가능하며 효과적인 협력적 대응체계를 구축하는 것임

5. 또한 해양 복합위협 국가전략과 대응체계의 효과적 운영을 위해 해양 복합위협을 정량적으로 평가할 수 있는 제도적 장치와 평가 정보를 포함한 위협의 예측 및 예방을 과학기술적으로 관리할 수 있는 정보분석 플랫폼의 구축을 정책제언으로 제시

요 약

해양 복합위협의 실효적 대응 방안 연구

민영훈 · 윤인주 · 임병호 · 황수연 · 조익순

1. 배경 및 필요성

- 한반도 주변 해역은 NLL 인접, 주요 해상교통로 밀집, 북·중·러 군사 활동 등으로 군사·비군사 위협이 중첩된 고 위험 해역으로 인식
- 해상 물류망·에너지 인프라·해저인프라·항만정보시스템의 디지털 의존도가 높아지며 물리·사이버·정보 영역이 결합된 복합위협 가능성이 증대하고 있음
- 기존 위기·재난·치안 체계는 위협 유형별·부처별로 분절되어 있어, 동시·연쇄적으로 발생하는 복합위협에 대한 통합 대응 역량이 미흡한 것으로 판단
- 이에 본 연구는 해양 복합위협의 국내·외 논의 동향과 주요 사례를 분석하여 해양 복합위협의 발생 경향과 유형을 도출하고 현재 이를 대응하기 위한 국낸 대응 체계 개선 방향을 제시함.
- 특히, 해양 복합위협을 대응하는 국내·외 대응 체계를 비교·분석하고,

해양 국제범죄 통계, GIS정보, 해양 복합위협 위험성 분석 등을 통해 국내 해양 복합위협 대응체계의 기능 및 관할의 중첩성을 확인하고, 국가 기능 및 자원의 효율적 관리와 실질적인 위협 대응을 위한 구체적인 방안을 제시함

2. 해양 복합위협의 이론적 검토 및 주요 사례 분석

1) 해양 복합위협 국내·외 논의 동향

- **유럽과 NATO를 중심으로 해양 복합위협에 대한 상당한 논의가 이루어지고 있으며, 특히, 유럽은 복합위협을 국가나 비국가 행위자가 특정 목표를 달성하기 위해 외교적, 군사적, 경제적, 기술적 수단 등 전통 및 비전통적 방법을 혼합하여 강제적·파괴적 활동을 자행하는 것으로 정의**
  - EU 집행위원회는 국가별 취약점을 도출하기 위해 위험성 평가를 개발과 위협과 관련된 사이버 정보 흐름을 모니터링하여 미연에 차단하기 위한 보안 위험 평가 모델 개발 추진 중
  - 복합 위협의 특징을 고려하여 다국적 정보 공유와 협력을 위한 유럽복합위협대응센터를 설립하고 해양 복합위협의 효과적 관리를 위한 분석과 다양한 정책적 방안 제시. 특히 해양 인프라 시설에 대한 위협을 해양 복합위협으로 정의하여 이를 대응하기 위한 다양한 정책 방안을 제시.
- **국내적으로는 밀입(출)국, 마약 밀수, 제재 무기 수송, 해양 사이버 위협 등 최근 발생하고 있는 해양 복합위협 사례를 중심으로 위협의 감시와 관리 실효적 대응에 관한 논의가 이루어지고 있음**
  - 정책 연구기관을 중심으로 범정부 차원의 협력적 체계 구축에 대한 논의가

이루어지고 있으며, 기술 및 안보 기관을 중심으로 사이버안보, 무인체계를 활용한 위협의 기술적 대응 방안이 논의되고 있음.

2) 해양 복합위협 범위 및 주요 사례 분석

- **해양 복합위협은 기존의 군사적·경제적 위험뿐 아니라 첨단기술 적용으로 인한 사이버 공격, 자율운항선박 관련 사고 및 테러의 활용, 해상물류 공급망 교란 등 다양한 새로운 위험으로 확대**
  - 복합위협은 대규모의 군사력을 사용하지 않고, 공격 주체의 노출을 최소화하며, 공격의도를 은폐하면서 전략적 목적을 달성하려는 무정형 전략으로 정의할 수 있으며, 해양 복합위협은 해양 또는 해양과 연계하여 발생하는 복합위협으로 정의할 수 있음.
  - 이러한 정의를 통해 해양 복합위협의 범위는 전통적인 유형으로서 해양 국제범죄와 해양테러, 신흥 유형으로 해양 사이버위협으로 구분할 수 있으며, 특히 이러한 위협들이 수단-행위로 연결되어 복합적인 형태로 나타나는 것을 해양 복합위협의 범위라고 할 수 있음.
- **해양 국제범죄 사례 분석을 통해 하나의 연속적인 사건에 다양한 정부 및 공공기관이 관할구역 및 대상에 따라 분산된 기능을 수행하고 있는 것을 확인할 수 있었으며, 광범위한 해양에서 다양하게 발생하는 해양 복합위협을 제한된 국가 자산으로 상시적으로 감시하는데 한계가 있음을 확인**
- **또한 해양테러와 해양 사이버위협 등 신흥 해양 복합위협의 경우, 개별 기관의 관할 및 기관의 역할에 따라 사후적 대응에 중점을 두어 사건을 대응하고 있음. 또한, 기관간 역할 조정 내지 협력 체계가 미흡하여 분절적으로 사건을 대응하고 있어, 대응 사각지대가 발생할 수 있으며, 예방적 대응이 쉽지 않음**

3. 해양 복합위협 대응체계 국외 사례 분석

1) 국가별 대응체계 특징 및 비교

- 미국은 공공안전과 보안, 국경과 이주, 기반시설, 경제부문을 주요 안보 위협 대상으로 분류하고 국토안보부 산하 해안경비대를 중심으로 세관국경보호청, 이민세관단속국, 연방비상관리청이 협력하여 물자, 사람, 재난 등의 유형별 위협에 유기적으로 기능을 통합하여 대응
- 일본은 해양 복합위협에 대해 영토분쟁을 수반하는 회식지대 상황에 무게를 두고 있으며, 특히 해양에서 발생하는 위협에 대해 국토교통성 산하 해사국의 항만국 통제를 제외하고 해상보안청이 관할 해역에서 발생하거나 영향을 미치는 위협을 초기 대응함
- 영국은 국경, 항만, 자유항, 사이버를 주요 대상으로 하여 수역, 항만과 선박, 글로벌 해운 항로에서 발생하는 해양 범죄와 해적, 테러, 사이버 위협 등을 주요 위협으로 고려. 개별 기관이 기능에 따라 사건을 대응하되 유기적인 체계가 유지될 수 있도록 관할을 명확히 구분하고 있으며, 범정부 차원의 국가 전략을 수립하고 합동해양안보센터를 통해 기능이 효율적으로 운영될 수 있도록 조정함

2) 국가별 대응체계 시사점

- 미국의 해양 복합위협 대응체계는 하나의 동일한 부처에 정보 및 대응 기관을 통합하여 모든 단계에서 유관기관이 연속성을 가지고 통합적으로 대응할 수 있는 대응체계를 유지
- 일본의 경우 유관기관의 소속과 역할이 분리되어 있지만 해양경비 전

담기관에 권한이 집중되어 신속한 초기대응이 가능하도록 하고 있음

- 특히, 정보수집부터 단속·체포, 수사까지 전 단계에 걸쳐 해양위협을 대응할 수 있는 기능을 해양경비 전담기관에서 수행하고 있음. 다만, 공간적으로 기능을 구분하여 해양에서 발생된 사건만을 대응함.

▪ **영국은 해양 복합위협 대응 기관의 역할이 정보 수집, 단속 체포, 형사 수사 등 단계별로 세분화되어 있지만, 개별 기관의 기능이 경비-관세-이민(경비 전담), 해상-육상 수사(수사 전담)으로 집중되어 수행할 수 있도록 제도적으로 세분화되어 있음.**

- 특히, 경비와 수사 전문적으로 구분하여 국가 자원을 효율적으로 활용하고 초기 대응과 사후 대응을 구분하여 기관간 기능이 유기적으로 연결되도록 제도화 하고 있음.

4. 해양 복합위협 국내 대응체계와 데이터 분석

1) 분절적 대응체계 및 책임의 모호성

▪ **본 연구는 국내 대응체계를 해양 복합위협의 유형인 해양 국제범죄, 해양테러, 해양 사이버 위협으로 구분하고, 이를 기능과 공간으로 구분하여 분석함.**

- 위협 유형별로 일련의 사건에 다양한 기관의 관할이 중첩되어 나타나는 것을 확인할 수 있었으며, 공간적으로 항만구역 등에서 관할의 모호성 내지 사각지대가 발생할 수 있음을 확인할 수 있음.

▪ **해양 복합위협 주요 발생 현황 및 경향을 분석하기 위해 해양 국제범죄 통계를 연도별 발생현황, 증감율, 변동성을 기준으로 분석하였으며, 이를 통해 밀수(출)입, 국민사회안전, 출입국문란이 우선적인 대응이**

필요한 해양 복합위협으로 확인됨.

- 해양 복합위협의 경우, 과거 발생 현황을 확인할 수 있는 통계가 국제해양범죄만으로 전체 해양 복합위협의 경향성을 도출하는 데는 한계가 있었으나, 밀수(출)입, 국민사회안전, 출입국문란 등과 관련된 주요 사례 분석을 통해 해양 복합위협이 국제화, 대형화, 전문화 되고 있음을 확인할 수 있었음.

▪ **해양 국제범죄의 발생과 관련 기관의 위치에 대한 GIS 분석을 통해 해양 복합위협 대응을 위한 국가 자원의 효과성을 분석하였으며, 이를 통해 원거리에서 발생하는 해양 국제범죄에 대한 자원 부족과 해양 복합위협 발생의 불확실성으로 인한 객관적인 데이터 확보, 대응체계의 통합적 구축 내지 국가 자원의 효율적 활용에 대한 필요성을 확인할 수 있었음.**

▪ **신흥 복합위협에 대한 위험성과 취약점을 확인하기 위해 미 해안경비대에서 적용하고 있는 MSRAM을 수정하여 우리 관할해역에서 발생할 수 있는 해양 복합위협의 위험성을 시범적으로 분석.**

- 다만, MSRAM의 경우, 위협요인을 위협발생가능성, 취약성, 영향으로 구분하여 다양한 정량적 데이터를 근거로 지수를 산정하나, 본 연구의 경우 해양위협에 대한 정량 데이터 확보가 어려워 개별 요인을 전문가 설문으로 계량화하여 산정.
- 본 연구는 위험성 분석을 통해 현재 국내적으로 드론 공격, 해저시설 공격, 사이버위협 등에 대한 대응 체계 마련이 정책 및 제도적으로 마련되어야 하는 것을 확인하였음.

5. 해양 복합위협의 실효적 대응 방안

1) 해양 복합위협 통합 대응체계 구축

- **해양 복합위협의 국내 대응체계의 중첩성과 모호성, 대응 사각지대를 해소하기 위해 다양한 기관의 기능을 통합적으로 조정하여 협력을 유도할 수 있는 통합 대응체계를 제시**

- 국외 대응체계 사례를 참조하여 우리나라 또한 다양한 기관의 기능을 조정할 수 있는 (가칭)국가해양위협대책위원회를 범부처 차원에서 설립하고 이를 통해 다양한 기관이 유기적으로 협력할 수 있는 체계를 확보
- 또한, 공간별로 해양 복합위협에 대한 신속한 대응을 위해 해양 법집행기관을 중심으로 초기 대응, 단속, 검거 등의 권한 행사가 일원화되어 행사되는 것이 필요. 이를 위해, 관련 정보 등을 통합해서 관리 및 운영할 수 있는 해양위협대응센터를 설립하여 위원회를 보좌하고 다양한 기관이 협력할 수 있는 플랫폼을 설립하는 것이 필요

2) 해양 복합위협 대응 국가전략 수립

- **해양 복합위협의 국제화, 대형환, 전문화를 고려하여 통합적 거버넌스를 효과적으로 운영하기 위해서는 해양 복합위협 대응 국가전략을 수립하는 것이 필요.**

- 이 전략은 해양 복합위협으로부터 국가 핵심이익을 보호하고 국가자원을 효율적으로 활용하기 위한 방안, 관계기관의 효과적인 협력 체계 구축을 위한 지침을 제공.
- 특히, 전략은 다차원적으로 발생할 수 있는 해양 복합위협을 예방-대비-대응-복구 등 발생 전 주기로 관리하고 국제 규범과 국내 법체계를 정합화

하며, 위험성을 기반으로 국가 자원을 효과적으로 배분할 수 있도록 구체적인 방향성을 제시하는 것이 필요

3) 해양 복합위협 위험성 평가 제도 도입

- **분석을 통해 해양 복합위협 발생의 비정형성을 확인할 수 있었으며, 이에 위협을 효과적으로 대응하기 위해서는 위험성에 기반한 과학적인 위협 대응이 필요.**
  - 미국, 영국, 호주 등 주요국은 해양 복합위협에 대응하기 위해 제도적으로 위험성평가를 도입하여 운용하고 있으며, 이러한 위험성 평가를 기반으로 국가 전략, 예산, 주요 정책 등을 수립하고 권역별로 대응을 위한 국가 자원을 배분함.
  - 이에 우리나라 또한 해양 복합위협을 효과적으로 대응하기 위해 주요국에서 도입하고 있는 위험성 평가제도를 참조하여 우리나라 해역의 특성과 해양 활동을 고려한 위험성 평가제도를 개발 및 도입하는 것이 필요

6. 결론 및 정책 제언

1) 요약 및 결론

- **본 연구는 최근 점차 확대되고 있는 해양 복합위협에 대한 국내적 대응체계를 진단하고 이를 개선하기 위한 방안을 제시하고 있음**
- **해양 복합위협의 비정형화, 국제화, 대형화, 전문화를 실효적으로 대응하기 위해 본 연구는 해양 복합위협 통합 대응체계 구축, 해양 복합위협 대응 국가전략 수립, 해양 복합위협 위험성 평가 제도 도입을 정책 방안으로 제시함**

2) 정책제언

- 본 연구는 분석을 통해 우리나라 현재 체계가 해양 복합위협을 실효적으로 대응하기에 다소 미흡한 것으로 확인하고, 특히, 발생 현안 별로 관련 기관의 분절적 대응이 관할의 중첩으로 이어지거나, 감시의 사각으로 연결될 수 있음을 확인했음

- 또한, 해양 복합위협의 비정형화, 국제화, 대형화, 전문화되는 것을 고려할 때, 위협의 예방 및 대비가 중요해짐에도 불구하고 마약 단속, 대테러 등 특정 분야의 협력체계를 제외하고 관련 기관간 포괄적 협력체계를 확인하기 어려워, 예방, 대비, 대응, 복구 등 전 주기에 걸친 실효적 대응 체계 수립이 필요한 것을 확인함

- 본 연구는 정책제언으로 통합적 거버넌스 및 국가전략의 제도화와, 해양 복합위협 위험성 평가 및 정보분석플랫폼 구축을 제시함.

  - 통합적 거버넌스 및 국가전략의 제도화는 해양 복합위협을 실효적으로 대응하기 위한 통합적 거버넌스를 제도적으로 구축하고 이를 이행하기 위한 국가 전략을 수립하여 지속가능하며 효과적인 협력적 대응체계를 구축하는 것임
  - 또한 해양 복합위협 국가전략과 대응체계의 효과적 운영을 위해 해양 복합위협을 정량적으로 평가할 수 있는 제도적 장치와 평가 정보를 포함한 위협의 예측 및 예방을 과학기술적으로 관리할 수 있는 정보분석플랫폼의 구축을 정책제언으로 제시

3) 후속과제

- 해양 복합위협이 지속적으로 증가하는 것을 고려하여 국내 해양 복합위협을 유형화하고 분류하여 통계적으로 관리하여 이를 위험성 평가

등 과학적 분석에 활용하는 것이 필요.

- 밀(입)출국, 밀수(출)입 등 전통적 해양 복합위협을 포함하여 다양한 형태의 위협에 대한 현황 및 통계의 정보 관리가 이루어지지 않아 해양 복합위협을 대응하기 위한 과학적이고 정책적인 대응방안을 수립하기가 어려움
- 이에, 해양 복합위협과 관련된 정보를 효과적으로 관리하기 위한 정보관리체계와 이를 데이터로 유지관리할 수 있는 정보관리시스템 구축이 필요

▪ **해양 복합위협에 대한 합리적 판단과 과학적 근거를 통한 객관적 정책 수립, 효율적 자원 배분 등을 시행하기 위해 해양 복합위협 위험성 평가 모델을 외국 사례등을 참조하여 개발 및 적용하는 것이 필요**

EXECUTIVE SUMMARY

A Study on Effective Countermeasures against Maritime Hybrid Threats

Young-Hun Min · In-Joo Yoon · Byeong-Ho Lim · Su Yeon Hwang · Ik-Soon Cho

1. Background and Necessity

- The seas surrounding the Korean Peninsula are recognized as high-risk maritime areas characterized by overlapping military and non-military threats. This risk profile stems from their proximity to the Northern Limit Line (NLL), the concentration of major sea lines of communication (SLOCs), and ongoing military activities by North Korea, China, and Russia.
- The increasing digital dependency of maritime logistics networks, energy infrastructure, subsea infrastructure, and port information systems has elevated the potential for hybrid threats that integrate physical, cyber, and information domains.

- Existing crisis, disaster, and public security systems are segmented by threat type and governmental jurisdiction, and consequently lack adequate integrated response capacity against hybrid threats that occur simultaneously or in cascading sequences.
- Accordingly, this study analyzes domestic and international discourse on maritime hybrid threats and examines key cases to identify occurrence patterns and typologies of such threats. Based on this analysis, the study proposes directions for improving Korea's response system to counter these threats.
- In particular, this study conducts a comparative analysis of domestic and international response frameworks for maritime hybrid threats. Through the examination of maritime transnational crime statistics, GIS data, and maritime hybrid threat risk assessments, it identifies functional and jurisdictional overlaps within Korea's current response system. Based on these findings, the study presents concrete measures for the efficient management of national functions and resources, as well as for practical threat response.

2. Theoretical Review and Case Analysis of Maritime Hybrid Threats

1) Domestic and International Discussions on Maritime Hybrid Threats

- Substantial discussions on maritime hybrid threats have been centered around Europe and NATO. In particular, Europe defines hybrid threats as coercive and destructive activities in which state or non-state actors employ a combination of traditional and non-traditional methods, including diplomatic, military, economic, and technological means, to achieve specific objectives.
  - The European Commission is developing risk assessment tools to identify country-specific vulnerabilities. It is also developing security risk assessment models that monitor threat-related cyber information flows to prevent attacks before they occur.
  - Recognizing the multifaceted nature of hybrid threats, the EU and NATO established the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) to facilitate multinational information sharing and cooperation. The Centre conducts analyses and proposes various policy measures for the effective management of maritime hybrid threats. Notably, it defines threats to maritime infrastructure as maritime hybrid threats and presents diverse policy responses to counter them.
- In Korea, discussions have centered on the surveillance,

management, and effective response to maritime hybrid threats, focusing on recent cases such as illegal border crossings, drug smuggling, transport of sanctioned weapons, and maritime cyber threats.

- Policy research institutions have led discussions on establishing whole-of-government collaborative frameworks, while technology and security agencies are exploring technical countermeasures leveraging cyber security and unmanned systems to address these threats.

2) Scope and Case Analysis of Maritime Hybrid Threats

- Maritime hybrid threats now extend beyond conventional military and economic risks to include cyberattacks enabled by advanced technologies, incidents and terrorist exploitation involving autonomous vessels, and disruptions to maritime supply chains.

- Hybrid threats can be defined as amorphous strategies that seek to achieve strategic objectives without deploying large-scale military forces, while minimizing exposure of attacking actors and concealing their intentions. Maritime hybrid threats can accordingly be defined as hybrid threats occurring in or in connection with the maritime domain.

- Based on this definition, the scope of maritime hybrid threats can be categorized into traditional types, which include transnational maritime crime and maritime terrorism, and

emerging types, specifically maritime cyber threats. Notably, maritime hybrid threats encompass situations where these threats manifest in compound forms through the integration of various means and actions.

- Analysis of international maritime crime cases demonstrates that multiple government and public agencies perform dispersed functions according to their respective jurisdictions and areas of responsibility within a single continuous incident. This analysis also confirms the limitations of maintaining constant surveillance over diverse maritime hybrid threats occurring across vast ocean areas with limited national assets.
- Furthermore, in cases of emerging maritime hybrid threats such as maritime terrorism and maritime cyber threats, individual agencies respond to incidents primarily through reactive measures based on their respective jurisdictions and institutional roles. Weak inter-agency role coordination and collaborative frameworks result in fragmented responses, creating potential blind spots and hindering proactive prevention efforts.

3. Analysis of International Cases of Maritime Hybrid Threat Response Systems

1) Characteristics and Comparison of National Response Systems

- The United States classifies public safety and security, border and immigration, infrastructure, and economic sectors as primary security threat targets. Centered on the U.S. Coast Guard under the Department of Homeland Security (DHS), the U.S. Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and Federal Emergency Management Agency (FEMA) collaborate through organically integrated functions to address type-specific threats involving goods, people, and disasters.
- Japan's approach to maritime hybrid threats emphasizes gray zone situations involving territorial disputes. Specifically, regarding threats occurring at sea, the Japan Coast Guard (JCG) conducts initial responses to threats occurring in or affecting jurisdictional waters, with the exception of Port State Control functions administered by the Maritime Bureau under the Ministry of Land, Infrastructure, Transport and Tourism (MLIT).
- The United Kingdom identifies borders, ports, freeports, and cyberspace as primary targets, with maritime crime, piracy,

terrorism, and cyber threats occurring in territorial waters, ports and vessels, and global shipping routes as principal threats. Individual agencies respond to incidents according to their respective functions, while jurisdictions are clearly delineated to maintain an organic system. The UK establishes whole-of-government national strategies and coordinates efficient operational functions through the Joint Maritime Security Centre.

2) Implications from National Response Systems

- The United States maintains a coordinated maritime hybrid threat response system by consolidating intelligence and operational agencies under a single government department. This structure enables relevant agencies to respond in an integrated and continuous manner throughout all stages of incident management.
- In Japan, while relevant agencies have separate jurisdictions and roles, authority is concentrated in a dedicated maritime security agency to enable rapid initial response.
  - Specifically, the dedicated maritime security agency (the Japan Coast Guard) performs functions capable of responding to maritime threats across all stages, from intelligence gathering to enforcement and arrest, and investigation. However, its mandate is geographically defined, responding only to incidents occurring within maritime domains.

- In the United Kingdom, maritime hybrid threat response agencies have roles segmented by operational stages such as intelligence gathering, enforcement and arrest, and criminal investigation. However, individual agencies are institutionally organized to concentrate their functions in distinct areas: border security operations (covering customs, immigration, and maritime border control) and investigative operations (covering both maritime and land-based criminal investigations).
  - In particular, the UK institutionalizes a clear functional distinction between security and investigative operations to optimize the allocation of national resources, while differentiating initial response from post-incident response to ensure seamless inter-agency coordination.

4. Korea's Response System to Maritime Hybrid Threats and Data Analysis

1) Fragmented Response System and Ambiguity in Responsibilities

- This study categorizes Korea's response system according to three types of maritime hybrid threats, specifically maritime transnational crime, maritime terrorism, and maritime cyber threats, and analyzes them from both functional and spatial

perspectives.

- The analysis reveals that jurisdictions of multiple agencies overlap across sequential incidents for each threat type. Additionally, jurisdictional ambiguities and blind spots can emerge in certain spatial areas such as port zones.

▪ To analyze the major occurrence patterns and trends of maritime hybrid threats, this study examined maritime transnational crime statistics based on annual occurrence status, growth rates, and volatility. This analysis identified smuggling, threats to public safety, and immigration violations as maritime hybrid threats requiring priority response.

- Available statistical data on past occurrences were limited to international maritime crime, which presented constraints in deriving overall maritime hybrid threat trends. However, analysis of major cases involving smuggling, public safety threats, and immigration violations confirmed that maritime hybrid threats are becoming increasingly internationalized, larger in scale, and more professionally organized.

▪ Through GIS analysis of maritime transnational crime occurrences and the locations of relevant agencies, this study assessed the effectiveness of national resource allocation for maritime hybrid threat response. The analysis revealed critical gaps: insufficient resources for addressing maritime transnational crimes occurring in remote areas, limited objective data due to the unpredictable nature of maritime

hybrid threats, and the need for establishing integrated response systems and more efficient utilization of national resources.

- To identify risks and vulnerabilities associated with emerging hybrid threats, this study adapted the Maritime Security Risk Analysis Model (MSRAM) employed by the U.S. Coast Guard to conduct a pilot risk assessment of maritime hybrid threats potentially occurring in Korean jurisdictional waters.
  - However, while MSRAM calculates risk indices based on diverse quantitative data by categorizing threats into likelihood, vulnerability, and consequence, this study quantified these individual factors through expert surveys due to the difficulty of obtaining quantitative data on maritime threats.
  - The risk assessment confirmed that Korea currently lacks adequate policy and institutional frameworks to address drone attacks, attacks on subsea infrastructure, and cyber threats, highlighting the urgent need to establish such systems.

5. Effective Countermeasures against Maritime Hybrid Threats

1) Establishing an Integrated Response System for Maritime Hybrid Threats

- To resolve the overlaps, ambiguities, and response blind

spots within the domestic response system for maritime hybrid threats, this study proposes an integrated response system capable of comprehensively coordinating functions across multiple agencies and facilitating inter-agency cooperation.

- Drawing on international best practices, Korea should establish a whole-of-government National Maritime Threat Response Committee (tentative name) that brings together multiple government departments. This would provide an institutional framework for effective inter-agency collaboration.
- To enable rapid spatial response to maritime hybrid threats, authority for initial response, enforcement, and arrest should be unified under maritime law enforcement agencies. To support this structure, a Maritime Threat Response Center should be established to integrate and manage relevant intelligence, assist the Committee, and serve as a collaborative platform for participating agencies.

2) Formulating a National Strategy for Maritime Hybrid Threat Response

- Given how maritime hybrid threats are spreading internationally, growing in scale, and becoming more sophisticated, Korea needs to develop a comprehensive national strategy to effectively operate its integrated governance system.
- This strategy would provide measures to protect national core

interests from maritime hybrid threats and efficiently utilize national resources, as well as guidelines for establishing effective cooperative frameworks among relevant agencies.

- In particular, the strategy must present concrete directions to manage multi-dimensional maritime hybrid threats across the full cycle of prevention, preparedness, response, and recovery; harmonize international norms with the domestic legal system; and allocate national resources effectively based on risk assessment.

3) Introducing a Maritime Hybrid Threat Risk Assessment System

- The analysis confirmed the irregular nature of maritime hybrid threat occurrences, highlighting the need for a scientifically-grounded, risk-based approach to effectively counter these threats.

- Major countries including the United States, the United Kingdom, and Australia have institutionally have institutionalized and operated risk assessment systems to address maritime hybrid threats. Based on these risk assessments, they formulate national strategies, budgets, and major policies, and allocate national resources for response by region.

- Accordingly, Korea should develop and implement a risk assessment system tailored to the characteristics of Korean waters and maritime activities, drawing on the frameworks adopted by these leading nations, to effectively address maritime

hybrid threats.

6. Conclusion and Policy Recommendations

1) Summary and Conclusion

- This study examines Korea's response system for maritime hybrid threats, which have been progressively expanding in recent years, and proposes measures for its improvement.
- To effectively respond to the irregular patterns, internationalization, large-scale expansion, and specialization of maritime hybrid threats, this study proposes the following policy measures: establishing an integrated response system for maritime hybrid threats, formulating a national strategy for maritime hybrid threat response, and introducing a maritime hybrid threat risk assessment system.

2) Policy Recommendations

- Through analysis, this study found that Korea's current system is inadequate for effectively addressing maritime hybrid threats. In particular, fragmented responses by relevant agencies to individual incidents can lead to jurisdictional overlaps or create surveillance blind spots.
- Considering the irregular patterns, internationalization,

large-scale expansion, and specialization of maritime hybrid threats, prevention and preparedness are becoming increasingly critical. However, excluding cooperative frameworks in specific areas such as narcotics enforcement and counter-terrorism, it is difficult to identify comprehensive inter-agency cooperative frameworks. This highlights the necessity of establishing an effective response system spanning the full cycle of prevention, preparedness, response, and recovery.

- This study proposes the following policy recommendations: institutionalization of integrated governance and a national strategy, and establishment of a maritime hybrid threat risk assessment system and information analysis platform.
  - To be specific, the institutionalization of integrated governance and a national strategy entails establishing an integrated governance framework to effectively address maritime hybrid threats and developing a national strategy to operationalize this framework, thereby creating a sustainable and effective collaborative response system.
  - To ensure effective operation of the national strategy and response system for maritime hybrid threats, this study proposes establishing institutional mechanisms for quantitative risk assessment. It also recommends constructing an information analysis platform capable of scientifically managing threat prediction and prevention by integrating assessment data and other relevant intelligence.

3) Follow-up Tasks

- Given the continuous increase in maritime hybrid threats, it is necessary to categorize and classify Korea's maritime hybrid threats for statistical management and utilize this data for scientific analysis, including risk assessment.
  - Korea lacks a comprehensive system for managing information on the current status and statistics of various maritime hybrid threats, including traditional threats such as illegal border crossings and smuggling. This deficiency makes it difficult to develop scientific and evidence-based countermeasures.
  - Therefore, it is essential to establish an information management framework for effectively managing maritime hybrid threat-related information and to construct an information management system capable of maintaining and utilizing this data.
- To enable rational decision-making, evidence-based policy formulation, and efficient resource allocation for maritime hybrid threats, it is necessary to develop and apply a maritime hybrid threat risk assessment model by referencing international cases.

01
서론

제1절 연구 필요성 및 목적

1. 연구 배경 및 필요성

최근 우리나라 주변 해역에는 다양하고 복합적인 위협이 동시다발적으로 발생하고 있다. 특히, 최근 급속하게 증가하고 있는 해상을 통한 대형 마약 유입, 드론 등 무인체계를 이용한 해양 주요시설 위협, 자율운항선박(MASS: Maritime Autonomous Surface Ship) 등에 대한 사이버위협 등은 국가적, 사회적, 경제적으로 막대한 영향을 미칠 수 있어 새로운 방법의 대응 방안을 요구한다. 그리고 이러한 새로운 해양위협에 더해 주변 해역의 외국선박 불법조업, 주변국과의 중첩수역 관할 문제, 불법 밀입(출)국, 허가받지 않은 물품의 밀수(출)입 등은 점차 고도화되어 기존 단속 방법의 개선을 요구한다.[1)]

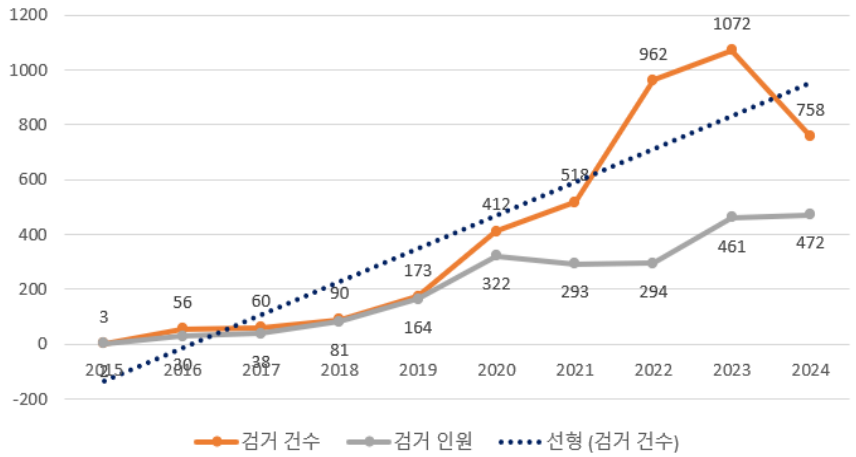
지정학적으로 우리나라 관할 해역은 서쪽, 남쪽, 동쪽으로 중국, 일본, 러시아와 중첩하고 있고, 북으로는 북방한계선(NLL: Northern Limit

1) 인천일보(2024.9.9.)(검색일: 2025.9.2.)

Line)[2]을 두고 있어 다양한 전통·비전통 위협에 노출되어 있다. 특히, 우리나라는 직접적으로 해양에서의 불법행위 및 위협에 노출되어 있는 동시에, 3면 모두 관할 해역 미획정 구역으로 직간접적인 안보 위협에도 노출되어 있다.

전통적 위협 외에도 최근에는 비전통 해양위협이 증가하고 있다. 최근 급속히 증가하고 있는 해양위협 중 사회·경제적인 영향과 파급효과가 가장 큰 것은 해양을 통한 대형 마약 유통이다. 이러한 마약 밀수는 코로나 팬데믹 이후 2023년부터 크게 증가하고 있는 것으로 보인다.

〈그림 1-1〉 해양경찰청 마약사범 단속 현황(2015년~2024년)



자료: 공공데이터포털(2025.3.18.)(검색일: 2025.4.28.)

2) 북방한계선은 1953년 8월 30일 당시 유엔군 사령관이었던 마크 클라크(Mark W. Clark) 장군이 설정한 대한민국과 북한의 서해 및 동해 접경 지점의 경계선이다. 아군 함정 및 항공기 초계활동의 북방한계를 규정해 남북 양측 간에 일어날 수 있는 충돌을 방지한다는 정전협정의 실질적인 이행에 목적을 두고 있는 사실상의 해상경계선이자 군사분계선이다. 서해상에는 당시 영해 기준 3해리를 고려하고 서해 5개 도서(백령도, 대청도, 소청도, 연평도, 우도)와 북한지역의 개략적인 중간선을 기준으로 '북방한계선'을 설정하였다. 동해상에는 군사분계선(MDL) 연장선을 기준으로 하여 '북방경계선(NBL: Northern Boundary Line)'을 설정하였다. 이후 1996년 7월 1일 「유엔사/연합사 정전시 교전규칙」을 개정하면서, 동·서해에 모두 '북방한계선(NLL)'으로 명칭을 통일하여 오늘에 이르고 있다. 보다 상세한 사항은 행정안전부 국가기록원(2017.12.26.)(검색일: 2025.8.31.) 참조

특히, 최근 해양을 통한 마약 밀수는 대형화되고 있어 한 번의 사고가 상당한 규모의 사회적 파급력을 가진다. 예를 들어, 2025년 4월 강릉 옥계항에 정박한 노르웨이 국적 일반화물선에서 발견된 코카인 2톤은 마약 단속 이래 사상 최대 규모의 적발량이다. 적발된 마약은 시가로 1조 원 상당이며, 우리나라 전체 인구보다 많은 6천7백만 명이 동시에 투약이 가능한 양이다.

〈표 1-1〉 국내 주요 해상 마약 단속 사례

장소	시기	내용	규모
강원도 강릉 옥계항	2025.4.	• 멕시코를 출항해 옥계항에 입항한 노르웨이 선적 화물선에서 코카인 약 2톤 적발 • 코카인 의심 물질 20~30㎏ 상장 57개를 발견	• 시가 1조 원 상당으로 6천7백만 명 동시 투약 가능 규모
강원도 공장	2024.8.	• 캐나다 범죄 조직으로부터 유입된 코카인 60㎏ 압수 • 국내 유통단계에서 적발된 코카인 중 최대 규모	• 시가 1천800억 원대 액상 마약으로 200만 명이 동시 투약 가능한 양
부산신항	2024.4.	• 미국발 화물선의 냉동 컨테이너에서 코카인 33㎏ 적발	• 시가 165억 원 상당
부산신항	2024.1.	• 브라질에서 출항하여 부산신항으로 입항한 우리나라 국적선 씨체스트에서 코카인 100㎏ 적발	• 시가 3천5백억 원 상당(약 330만 명 동시 투약 가능)
부산신항	2020.12.	• 부산신항 화물선에서 코카인 25㎏ 적발	• 시가 1천억 원 상당
충남 태안항	2019.8.	• 태안항 화물선에서 코카인 100.764㎏ 적발	• 시가 3천억 원 상당
부산신항	2017.11.	• 부산신항 화물선에서 대마 150㎏ 적발	• 시가 75억 원 상당

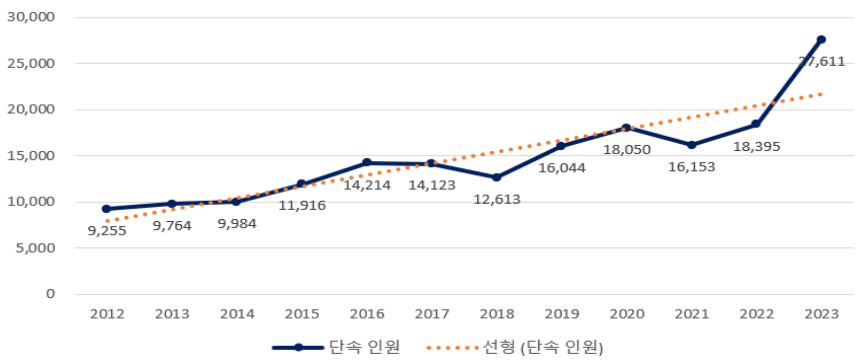
자료: 연합뉴스(2025.4.2.)(검색일: 2025.4.28.); 연합뉴스(2024.8.19.)(검색일: 2025.4.28.); KBS뉴스(2024.6.20.)(검색일: 2025.4.28.); KBS뉴스(2024.1.16.)(검색일: 2025.4.28.); 연합뉴스(2023.4.9.)(검색일: 2025.4.28.) 참조하여 저자 작성

2016년 "마약류 등 유해약물의 사회적 비용 분석" 연구는 마약류 등 유해약물의 사회적 비용을 약 2조 2,390억 원(암수율 고려)으로 추산했다. 연도별 마약류 사범 단속 인원이 2016년 14,214명에서 2023년 27,611명으로 두 배 가까이 증가한 것을 고려할 때, 2023년 마약 오남용으로 인한 사회적 비용은 단순 계산만으로도 2조 원의 두 배 이상이 될 것으로 예상

된다.[3] 다만, 2023년 마약류 등 유해약물로 인한 사회적 비용을 마약류 사범 단속 인원에만 근거하여 추계하는 것은 어려울 것으로 판단된다. 그럼에도 불구하고 이러한 단속 인원의 증가는 상당한 가능성으로 막대한 사회적 비용의 증가로 연결된다.

이러한 마약류의 80% 이상이 선박 등 해양을 통해 유입된다는 사실은 마약 밀수의 경로가 다양화되고 수단이 고도화되며, 행위자는 조직화 및 정밀화되고 있다고 할 수 있다. 또한, 이러한 마약 밀수는 최근 단속이 엄격한 국가 무역항에서 벗어나 지방 무역항, 또는 일반 연안 지역으로 경로가 다양화되고 있다.[4] 해상 마약 밀수는 한 번에 대량의 마약 유통으로 이어질 수 있는 만큼 효과적인 예방 및 단속이 이루어져야 하고 이를 위해서는 전문적인 대응체계 및 정책적 방안이 요구된다.[5]

〈그림 1-2〉 연도별 마약사범 단속 현황(2012년~2023년)



자료: 한국마약퇴치운동본부(2022)(검색일: 2025.4.28.); 뉴스1(2024.2.9.)(검색일: 2025.4.28.) 참조하여 저자 작성

3) 박성수(2018), pp. 233-244. 이 연구에서는 마약류 등 유해약물의 사회적 비용을 의료비용, 생산성 비용, 형사사법비용, 주변고통비용으로 구분하여 추계하였음. 따라서 2023년 마약류 사법 단속 현황만을 근거로 관련 사회적 비용을 추계하는 것은 실제로 어려울 것으로 판단됨

4) 연합뉴스(2025.4.15.)(검색일: 2025.4.28.)

5) 연합뉴스(2023.12.7.)(검색일: 2025.4.28.) 이 뉴스에 따르면, 2021년 국내 주요 마약류 밀반입 압수량은 총 1,016㎏이며, 이 가운데 선박을 이용해 밀반입하다 적발된 양은 837㎏에 달함; 연합뉴스(2024.8.19.)(검색일: 2025.4.28.) 이 뉴스에 따르면, 해상을 통해 유입된 대량의 마약 원료가 국내에서 가공되어 국제 범죄조직을 통해 국외로 유통될 가능성을 시사하고 있음.

또한 해양의 대표적 위협 형태인 해상 밀입(출)국은 최근 그 동기와 수단이 다변화 및 고도화되고 있다. 과거 경제적 어려움을 극복하기 위해 다수의 해상 밀입(출)국이 대부분 발생했다면, 최근 밀입(출)은 경제적 이유를 비롯하여, 정치적 불안정 및 인권 침해 탈출, 범죄 도피, 정보 활동 등 다양한 이유로 발생하고 있다. 특히, 주로 대형 상선 등을 통해 시도되었던 과거의 밀입(출)국이 무역항의 단속 강화로 소형보트, 제트스키 등을 이용한 연안 지역 밀입(출)국 시도로 변화하고 있으며, 이러한 시도는 2024년 이후 증가추세에 있는 것으로 보인다.[6] 관련 기관은 변화와 증가 추세에 대비하기 위해 지역별 전담반을 조직해 취약 시간대 경비를 강화하고 있으나 자원의 한계와 기관 간 분절적 대응으로 효과적인 단속에 한계를 겪고 있는 것으로 판단된다.

〈표 1-2〉 최근 주요 밀입(출)국 시도 사례

사건 개요	시기	내용	특징
인천 소청도 밀입국 시도	2025.2.	• 중국 산둥에서 고무보트를 타고 인천 옹진군 소청도 인근 해상으로 밀입국 시도	• 어선안전조업국을 통해 선박 접근 사실을 해양경찰에서 접수 • 중국인 두 명이 해양경찰에 의해 검거된 사건으로 과거 불법체류로 강제퇴거된 전력이 있음
서귀포항 밀출국 사건	2024.1.	• 영풍제지 주가조작 사태 주범이 어선 창고에 숨어 베트남으로 밀항 시도	• 밀항자 신고를 통해 해양경찰 단속 • 선박 알선, 현지 입국 등과 관련한 국제조직 범죄 • 해양경찰 신고로 발견했으나 출입국관리 등에 관한 행정시스템 적용 누수 문제 지적
보령 연안 밀입국 사건	2023.10.	• 중국인 22명이 고성능 선박을 이용하여 보령 인근 해상까지 접근하여 바다를 통해 밀입국 시도	• 경찰청의 미확인 선박 신고를 통해 해양경찰청이 단속 • 수색 및 단속은 군, 경찰, 해양경찰이 함께 실시 • 중국 현지 조달책과 국내 조력자가 연결될 가능성이 있는 국제조직 범죄 • 관련 범죄에 관한 정보 수집 협력체계 미비

자료: 인천해양경찰서(2025.3.12.)(검색일: 2025.4.28.); 연합뉴스(2024.1.26.)(검색일: 2025.4.28.); 동아일보(2023.11.1.)(검색일: 2025.4.28.) 등을 참조하여 저자 작성

6) 연합뉴스(2025.10.6.)(검색일: 2025.10.30.) 등 밀입국 관련 최근 사건 참고.

특히, 최근 발생하고 있는 해상 밀입(출)국은 조직화, 체계화, 전문화, 국제화되고 있어, 사전 정보의 취득 없이는 인지 및 발견이 어렵다. 또한 조직화, 체계화, 전문화는 밀입(출)국의 수단이 되는 선박을 전문적으로 개조하거나 레이더 회피 장비 등을 설비하는 불법 개조까지 유도하고 있어 하나의 위법 행위 달성을 위해 여러 개의 위법 행위가 연결되는 현상으로 발전하고 있어 이에 대응하기 위한 기관 간의 협력이 요구된다.[7] 뿐만 아니라 밀입(출)국의 동기가 산업기밀 유출, 테러 등과 연계될 경우, 국가 안보 및 국익에 직접 영향을 미칠 수 있어, 무역항을 포함한 일반 연안에 대한 위협 관리 필요성 또한 높이고 있다.

〈표 1-3〉 주요 해양 국제범죄 발생 현황(최근 5년)

구분	2020년	2021년	2022년	2023년	2024년
출입국 단속	69	62	74	74	76
국익, 산업보호	11	3	3	4	4
인권보호	14	8	4	20	12
환경보존	31	50	28	26	27

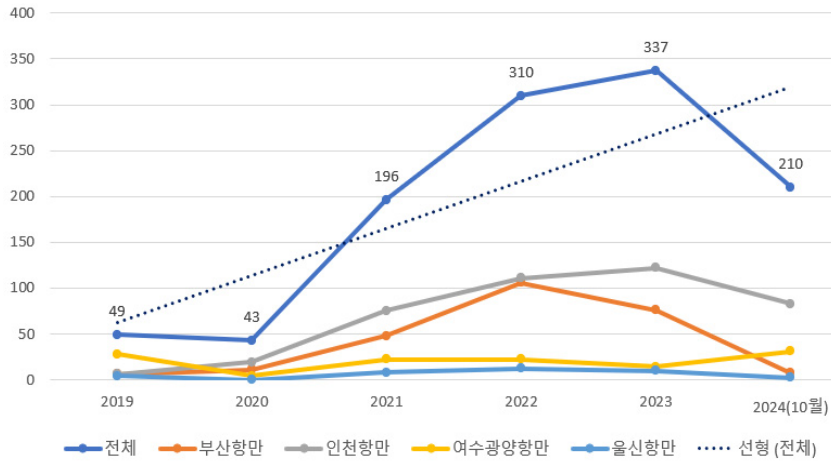
주: 전체 해양 국제범죄 중 출입국문란, 국익, 산업보호, 인권보호, 환경보존에 관한 범죄 현황만을 발췌하여 정리
자료: 해양경찰청(2025) 참조하여 저자 작성

이에 더해, 최근 디지털화, 무인화되고 있는 위협 수단은 전통적 위협인 테러 등과 결합하여 위협의 예방 및 대응을 어렵게 하고 있다. 예를 들어, 항만시설, 발전소 등 국가중요시설을 해킹하여 기능을 무력화하고 이후 드론 등을 통해 해안에 위치한 국가중요시설을 원거리에서 파괴하는 행위는 국가의 무역 기능을 일시적으로 마비시키거나 국가 에너지 공급망을 훼손시켜 사회적 혼란을 야기할 수 있다.[8] 이미 국내에서도 주요 항만시설에

7) 조민상(2023), pp. 220-221.
8) CSIS(2025)(검색일: 2025.9.2.); CSIS(2021.12.21.)(검색일: 2025.9.2.); CSIS(2019.8.5.)(검색일: 2025.9.2.) CSIS는 Brief와 보고서를 통해 이란 및 후티 무장 단체와 사우디아라비아의 전쟁 중 발전시설 및 주요 항만시설 공격에 사이버와 드론, 미사일 등이 활용된 사건을 분석하여 보고하고 있음

대한 사이버 침해 사고는 다수 확인되고 있으며, 항만시설 및 교량 등 주요 국가 인프라에 대한 드론 공격 또한 러시아-우크라이나 전쟁 등을 통해 확인이 가능하다. 특히, 항만 사이버 침해로 인한 정보 유출은 국가전략 물자에 관한 수출입 정보를 유출하여 국가 산업 또는 안보 전략에 막대한 영향을 미칠 수도 있다.[9)]

〈그림 1-3〉 연도별 해양시설 사이버 침해 현황



자료: 데일리안(2024.10.22.)(검색일: 2025.4.28.); 현대해양(2024.11.14.)(검색일: 2025.4.28.) 참조하여 저자 작성

2019년 사우디아라비아 아람코 석유 시설 드론 공격, 2023~2024년 후티 반군 무인수상정 선박 공격, 러시아 크림대교 수중 드론 테러 사건[10)] 등은 첨단기술 기반 위협의 위험성과 익명성을 여실히 보여준다. 더욱이 이러한 위협이 국가중요시설 및 주요 인프라인 항만시설, 해상 교량을 대

9) 하도연·김율성(2023), p. 438.

10) 연합뉴스(2019.9.16.)(검색일: 2025.4.28.); MBC뉴스(2024.1.5.)(검색일: 2025.4.28.); 서울뉴스(2023.7.17.)(검색일: 2025.4.28.) 등은 최근 드론 및 무인수상정 등 첨단기술을 활용한 선박 및 항만시설 공격이 사람과 물리적 수단을 동원한 전통 위협 행위를 대체하고 있는 것을 보여준다. 또한 이러한 무인체계를 이용한 위협 행위는 조정자의 위치와 드론의 위치를 분리시켜 실제 행위자의 위치를 확인하는 것을 어렵게 하여 원인을 밝히거나 단속하는 것을 어렵게 한다.

상으로 할 경우, 그 피해는 인명 피해와 더불어 막대한 경제적 피해를 유발한다. 특히 이러한 위협은 익명성을 전제로 하고 있어 위협의 존재만으로 사회 질서 혼란 등을 유도할 수 있다.

반면 이렇게 고도화 및 다양화되고 있는 해양위협에 비해 이를 예방하고 대비하기 위한 국가적 대응체계는 대상의 중첩성, 관할의 모호성 등으로 인해 위협에 대한 효과적 대응과 책임 있는 관리가 미흡한 실정이다. 현재 우리나라에서 해양위협에 대응하는 체계는 사후적 관리를 중심으로 기관의 관할과 대상에 따라 수립되어 있다.

예를 들어, 국가 관할권이 제한적으로 적용되는 배타적 경제수역(영해 기선으로부터 200해리)의 경우, 불법조업과 관련하여 주로 해양수산부와 해양경찰청이 불법행위를 대응하고 이를 단속한다. 접속수역(영해 기선으로부터 24해리)에서는 관세청, 출입국·외국인정책본부, 질병관리청 등이 관세, 출입국, 검역 등을 위해 관련 위반 행위를 단속한다. 영해에서 발생하는 위법행위 내지 일반적인 범죄행위는 주로 해양경찰청이 담당하고, 항만의 보안업무는 무역항의 경우 해양수산부의 지방해양수산청과 항만공사가, 일반항 및 연안의 경우 해양경찰청이 1차적으로 위법행위에 대응한다. 더불어 국제여객터미널의 출입국 및 밀수품 단속은 관세청과 출입국·외국인청이 관리하며, 같은 장소에서 해양경찰청은 치안 유지 업무를 담당한다. 그리고 연안여객터미널의 경우, 안전 유지 및 보안 등에 관한 사항을 「해운법」에 따라 한국해양교통안전공단이 담당한다.[11)]

즉, 관할별로 다양한 기관들이 광범위한 해양위협을 각자의 역할에 따라 분리하여 관리하고 있으며, 필요에 따라 특정 위협에 대해서는 기관 간 협력하는 방식으로 대응하고 있는 것이다. 최근 발생하고 있는 새로운 해양위협 또는 고도화된 범죄행위가 기관의 관할 구역 또는 대상을 넘어 발생

11) 보다 상세한 내용은 본 보고서 제4장 제1절 참조.

할 경우, 이러한 위협에 대응할 수 있는 일반적인 협력체계가 제도적으로 수립되어 있지 않다. 따라서 협력의 대상이 되는 마약범죄 등 특정 위협을 제외하고 일반적인 해양위협에 대해서는 해양경찰청, 경찰청, 해군 등 일반적인 안보 및 질서 유지 기관이 그 관할 구역에 따라 분절적으로 대응한다. 이에, 특정 관할 구역을 초월하여 발생하거나 사회적으로 큰 영향을 미치는 최근 해양위협에 효율적으로 대응하기 위해서는 현재의 제도적 한계를 보완할 수 있는 정책 개선이 필요하다.

2. 연구 목적

본 연구는 궁극적으로 최근 발생하고 있는 해양위협의 동향과 경향을 분석하고, 이러한 위협에 대응하는 현행 체계를 항만과 연안으로 구분하여 평가하고, 이를 개선하기 위한 정책적 수단을 제시하는 것을 목적으로 한다. 앞에서도 언급한 바와 같이 점차 국제화, 조직화, 고도화, 지능화, 강력화되는 해양위협에 대응하기 위해서는 최근 발생하고 있는 해양위협을 분석하고, 변화하고 있는 불법행위와 신흥 복합위협에 관한 동향 및 경향을 분석하여 이러한 위협에 대응하기 위한 정책을 도출하는 것이 필요하다.

이에 본 연구에서는 먼저 전통적 해양위협으로서 해양 국제범죄의 동향과 경향을 분석한다. 또한 신흥 해양위협으로 사이버와 첨단기술을 활용한 해양위협을 분석한다. 다만, 이들 위협에 관한 명확한 법적 정의와 학문적 정의가 부재하여 최근 이들 신흥 해양위협에 대한 논의 동향을 분석하여 우리나라가 대응해야 하는 주요 해양위협의 범위를 도출하고 이들에 대한 대응 방향 및 정책을 분석하고자 한다.

본 연구를 통해 도출된 결과는 5대 국정 목표 중 '기본이 튼튼한 사회'를 달성하는 데 활용될 것으로 기대된다. 정부는 본 국정목표 달성을 위해 여

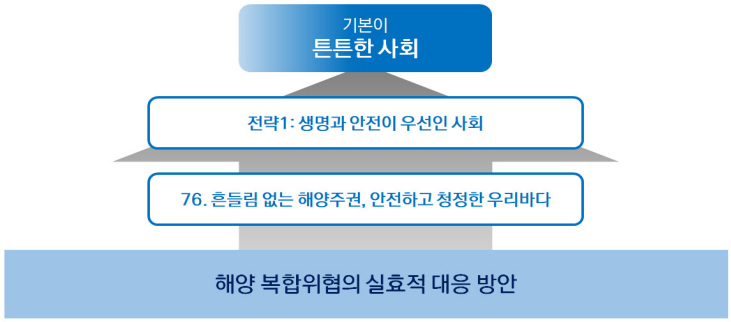
덟 가지 전략을 수립하고, 그중 '생명과 안전이 우선인 사회'를 제1전략으로 정하고 있다. 또한 정부는 이 전략의 달성을 위해 '76. 흔들림 없는 해양주권, 안전하고 청정한 우리바다'를 국정과제의 하나로 정하고 있어, 본 연구의 목적인 해양위협의 효과적 대응 방안 마련은 이러한 국정과제를 달성하는 데 활용될 수 있을 것으로 기대된다.

특히, 연안을 중심으로 거주하고 있는 520만 명(2023년 기준)의 국민은 해양으로부터 유입되는 위협에 직접적인 영향을 받는다.[12] 이들은 2021년 기준 우리나라 총생산의 36.6%를 감당하고 있으며, 지역적으로 약 704조 원을 담당한다.[13] 따라서 육지 및 해양을 통해 연안으로 유입되는 위협을 효과적으로 관리하는 방안을 모색하고 관련 정책을 개선하는 것은 국가 경제를 안정적으로 유지하기 위한 필수적인 환경을 제공한다.

또한 국제범죄 등 해양위협을 실효적으로 대응하기 위한 정책 개선 방안은 흔들림 없는 해양주권을 수호하고, 안전하고 청정한 우리 바다를 확보하여 해양을 통해 경제생활을 영위하는 국민의 지속가능한 해양 이용을 보장하는 국정과제 전략을 지원한다.[14] 이에 본 연구를 통해 도출한 해양위협의 실효적 대응 방안과 정책 개선 방안은 해양위협을 효과적으로 관리하고 대응하는 협력적 국가 거버넌스를 구축하는 데 이바지하고 관련 국가정책을 실천하기 위한 정책자료로 활용될 것으로 기대된다.

12) 연안포털(검색일: 2025.4.28.)
13) 연안포털(검색일: 2025.4.28.)
14) 국정기획위원회(2025)

〈그림 1-4〉 본 연구의 목적과 정부 국정과제 연관성



자료: 국정기획위원회(2025), p. 1.를 참조하여 저자 작성

제2절 연구 범위 및 방법

1. 연구 범위 및 주요 내용

본 연구의 범위는 우리나라 관할 해역에서 발생 가능한 해양위협을 대상으로 한다. 다만, 최근 해양위협은 앞에서도 살펴본 바와 같이 다양화·고도화되고 있으며, 관할 구역과 피해의 범위가 넓고 수단과 방법 또한 복합적으로 나타난다.

이에 본 연구에서는 최근 우리나라 관할 해역 및 관할권이 미치는 영역에서 발생하고 있는 위협을 '해양 복합위협'으로 명명하고, 이에 대한 범위를 전통적인 '해양 국제범죄', 신해양위협으로 '해양테러' 및 '해양 사이버위협'으로 구분하여 분석하고자 한다.

다만, 현재 본 연구에서 가용한 통계자료는 해양경찰청에서 관리하는 밀수(출)입, 밀입(출)국 등과 관련된 국제범죄 적발 통계다. 이에 본 연구에서

해양 복합위협의 데이터 분석 대상은 해양 국제범죄로 한정하여 수행한다. 더불어 해양 복합위협과 관련 기관의 연계성을 분석하기 위해 국제범죄의 발생 위치와 유관기관의 사무소 위치의 상관관계를 분석하고자 한다.

다만, 해양 복합위협의 위험성 분석은 우리나라 관할 해역에서 발생 가능한 위협을 모두 포괄한다. 외국 사례 및 전문가 자문 등을 통해 해양위협을 유형화하고 이렇게 도출된 해양위협의 유형에 대한 국내외 대응체계를 분석하고 개선 방안을 제시하고자 한다. 이는 해양 복합위협의 효과적 대응을 위해서 전통적인 위협인 해양 국제범죄를 포함하여, 신흥 위협인 해양테러, 해양 사이버위협 등에 대해서도 적절한 정책적 대응 방안과 협력적 거버넌스 개선이 필요하기 때문이다.

우리나라 국가정보원은 국제범죄 차단을 주요 업무 중 하나로 정하고 있으며 마약, 위폐, 불법입국, 보이스피싱 등과 같은 국제범죄를 안보 위협 요소 등으로 정하고 국내외 수사기관들과 긴밀하게 협력하고 있다.[15] 또한, 해양경찰청은 해양에서 발생하는 국제범죄를 직접 단속하거나 관세청, 법무부 출입국·외국인청과 협력하여 관련 범죄를 수사 및 조사, 처벌한다.[16]

따라서 본 연구는 이들 기관에서 관리 및 대응하고 해양 복합위협의 현황을 분석하고 이에 대응하는 기관의 협력체계 등 거버넌스를 진단 및 평가한다. 특히, 최근 신흥 안보 위협으로 여겨지고 있는 첨단기술을 활용한 미래 복합위협을 분석하기 위해 새롭게 등장하고 있는 위협 사례 또한 전통 해양 복합위협 사례에 더하여 분석한다. 이를 통해 본 연구는 해양 복합위협의 특성과 쟁점을 분석하고, 위협에 대응하기 위한 관련 기관의 협력적 거버넌스에 대한 시사점을 도출하고자 한다.

본 연구의 흐름은 다음과 같다. 이어지는 제2장은 해양 복합위협에 대한

15) 국가정보원, 국제범죄(검색일: 2025.4.28.)
16) 해양경찰청(2025.2.6.)(검색일: 2025.4.28.), p. 10 등 참조

이론적 검토와 사례 분석을 다룬다. 해양 복합위협을 정의하고 유형별 주요 사례를 통해 실효적으로 대응해야 할 필요성을 도출한다. 이어지는 제3장에서는 실효적 대응방안 수립에 참고할 수 있는 국외 사례로 미국, 일본, 영국의 대응체계를 분석한다. 제4장에서는 국내 대응체계와 실제 해양 복합위협 발생 현황 및 위험성 평가 분석을 수행하고, 국내 대응체계의 한계와 정책 우선순위를 도출한다. 제5장에서는 이러한 한계를 극복하고 정책 우선순위에 대응하기 위한 개선 방안을 제시한다. 마지막으로 제6장에서는 연구의 결론으로 본 연구를 통해 제시하고자 하는 정책을 제언하고 연구의 한계를 근거로 후속과제를 제안한다.

제2장은 연구 범위 및 대상의 객관적 범위 설정을 위해 해양 복합위협에 관한 정의 및 범위를 이론적으로 검토한다. 기존 해양위협이 신흥 위협과 더불어 복합적으로 나타나고 있어 이에 관한 국내외 논의 동향을 살펴본다. 이를 토대로 해양 복합위협의 개념과 정의를 도출하고, 범위와 유형을 구분한다. 나아가 해양 복합위협을 해양 국제범죄, 해양테러, 해양 사이버위협으로 구분하고 주요 사례를 분석한다.

제3장은 해양 복합위협에 대응하는 주요 국가의 관리제도 및 거버넌스를 검토한다. 효과적인 대응을 위해 주요국들이 채택 및 구축하고 있는 국가별 유관기관 간 협력체계와 정책 수단을 비교·분석한다. 특히, 전 세계적으로 해양 복합위협을 가장 포괄적으로 대응하고 있는 미국의 대응체계와 관련 제도를 분석하고, 기관들의 역할을 분석하여 우리나라 관할 해역에서 발생하는 위협에 효과적으로 대응하기 위한 정책적 시사점을 도출한다. 또한 주변국으로서 우리나라와 유사한 해양위협에 처해있는 일본의 관련 대응 정책과 거버넌스를 검토 및 분석하여 우리나라 관련 정책에 관한 시사점을 도출한다. 이와 더불어, 전통적 해양 강국이면서 유럽 해양 복합위협 체제의 중심적 역할을 하는 영국의 해양위협 대응체제를 검토하여 우리나라 관련 기관들의 위협 대응을 위한 협력체계 구성에 관한 시사점을 도출한다.

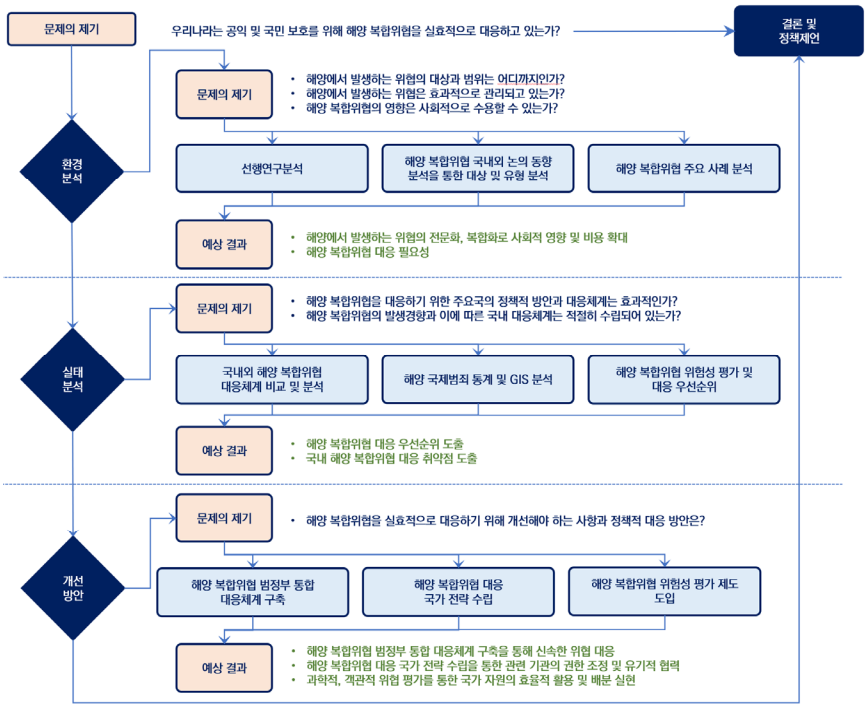
제4장에서는 최근 해양 복합위협의 경향, GIS 분석 등을 통한 취약지역 등을 근거로 국내 해양 복합위협 관리제도 및 대응 거버넌스를 분석한다. 먼저, 국내 기관에서 해양 복합위협에 대응하기 위해 추진하고 있는 정책을 분석한다. 다음으로, 해양 복합위협 발생 현황을 분석하기 위해 해양 국제범죄 통계분석을 실시한다. 또한 해양 복합위협의 취약지역 및 환경적 특징을 분석하기 위해 관련 범죄의 발생 위치와 관련 기관과의 상관관계를 분석하고 시사점을 도출한다. 마지막으로 미래 해양 복합위협의 위험성을 분석하여 정책 우선순위를 도출한다.

제5장에서는 제4장에서 도출된 국내 대응체계의 한계와 데이터 분석 시 사점을 근거로 이를 개선하기 위한 정책 방안을 제시한다. 특히, 해양 복합위협을 효과적으로 대응하기 위해 국가적으로 통합 대응체계를 구축해야 할 것과 해양 복합위협 대응을 위한 국가전략 수립, 위험성 평가 제도 도입을 정책 방안으로 제시한다. 이는 과학적이고 객관적인 국가 평가 체계를 통해 국가자원을 효율적으로 활용하고, 위협의 사각지대를 최소화하여 실질적인 위협 대응이 이루어지도록 하기 위함이다. 특히 해양 복합위협이 국제화, 다양화, 대형화, 복합화 되고 있는 가운데, 이러한 위협에 대한 실효적 대응이 적절히 이루어지지 않을 경우, 대형 피해와 복구 비용이 사회적 부담으로 작용할 수 있다. 이에 제5장에서는 이러한 피해를 최소화하기 위한 효율적인 국가 체계와 이를 운영하기 위한 제도를 앞서 언급한 세가지 방향을 중심으로 제언한다.

제6장에서는 분석을 통해 도출된 문제점과 이를 해결하기 위한 해양 복합위협의 실효적 대응 방안을 중심으로 결론을 제시하고 정책제언으로 통합적 거버넌스 및 국가전략의 제도화, 해양 복합위협 위험성 평가 및 정보분석플랫폼을 구축할 것으로 제시한다. 이와 더불어, 후속과제로서 해양 복합위협 관련 정보 수집 및 관리 체계 구축 연구, 해양 복합위협의 위험성을 구체적으로 평가하기 위한 모델 개발 연구가 추진되어야 할 것을 본 연구

의 한계와 더불어 제시한다.

〈그림 1-5〉 연구 추진체계



자료: 저자 작성

2. 연구 방법

본 연구는 복합적이고 다면적인 특성을 가진 연구 대상인 해양 복합위협을 분석하기 위해 정량적 분석과 정성적 분석을 교차적으로 활용하는 혼합적 연구 방법(mixed research methods)을 적용한다. 정량적 방법은 해양 국제범죄 발생 통계, 단속 실적, 관련 기관의 감시 시스템의 관할 범위 등 정량적 데이터를 객관적인 문제 진단과 대응 효과성을 평가하기 위해

적용한다. 특히, GIS 기반의 공간 분석과 시계열 분석을 통해 해양 복합위협의 유형별, 지역별, 시간대별 분포를 파악하고 위협 발생의 취약 장소를 도출한다. 뿐만 아니라, 위험성 평가를 통해 유형별 해양 복합위협에 대한 위험을 도출하고 우리나라 관할 해역에서 우선적으로 대응해야 하는 해양 복합위협을 도출한다.[17]

정성적 방법은 해양 복합위협의 복잡한 성격과 다양한 기관 간의 상호작용을 심층적으로 이해하고 분석하는 데 유리하다. 특히, 해양안보 전문가, 해양경찰, 관련 부처 공무원, 공공기관 등의 자문을 통해 현행 대응체계의 한계와 개선 필요성을 도출할 수 있다. 이러한 관점에서 국내외 해양 복합위협과 대응체계에 관한 정책자료 등 문헌연구를 수행하고, 관련 주요 사례에 관한 전문가 자문, 표적집단면접법(Focus Group Interview)을 실시하고자 한다.

또한 유형별 해양 복합위협의 주요 사례에 대한 원인, 대응 현황, 효과 등을 분석하여 현재의 해양 복합위협 대응체계의 쟁점과 개선 방향을 도출하고자 한다. 이를 위해 국내외 사례와 해양위협 대응체계 및 정책 현황을 검토한다. 국내외 사례 분석을 바탕으로 우리나라 해양위협 관리제도의 취약점을 분석하고 이를 개선하기 위한 방향을 도출한다. 현재 해양에서 발생하는 해양위협은 앞에서도 언급한 바와 같이 주로 개별 기관이 관할 구역 및 대상에 따라 대응하거나 일부 위협에 대하여 유관기관과 협력을 통해 대응한다. 이에 해양위협 대응 거버넌스와 협력체계 운영에 관한 실효성 등을 확인하기 위해 관련 부처와의 정책실무협의회, 자문회의, 인터뷰 등을 실시하고 관련 논의를 바탕으로 정책적 시사점을 도출한다.

아울러, 항만시설의 보안 실무와 연안에서 발생하는 국제범죄를 실제 단속 및 대응하는 해양경찰서, 항만공사, 항만보안공사, 법무부 출입국·외국

17) 박민석 외(2024), p. 85. 이 논문은 위협 등에 관한 위험성 평가 시행이 안전사고 예방에 효과가 있고, 특히 산업별 특성과 사업장별 여건 및 규모에 맞추어 위험성 평가를 실시할 경우 그 효과가 향상한다는 것을 언급

인청, 관세청 등 관계기관으로부터 전문가 자문 및 의견 청취를 통해 변화하는 해양위협에 대응하기 위한 정책 및 법·제도 개선 방안을 도출하고 정책 실현화를 확보하고자 한다.

실제로 본 연구는 해양 복합위협 대응과 가장 관계가 많은 해양경찰청과의 정책협의회 및 자문을 실시하여 실효적 위협 대응을 위한 제도적 개선사항과 현장의 애로사항을 확인했다. 뿐만 아니라 본 연구는 당해 연구기간 동안 유관기관 및 관련 기관의 전문가에게 표적집단면접을 실시하고, 실제 해양 복합위협에 대응하는 업무와 관련하여 현장의 문제점을 확인했다. 또한 유사 연구를 수행한 선행 연구자 및 관련 전문가들과의 세미나를 실시하여 해양 복합위협 대응을 위한 제도상 문제점에 관한 시사점을 도출할 수 있었다. 마지막으로 해양 보안 및 위협과 관련된 데이터 및 GIS 분석을 진행한 전문가에게 자문을 받아 위협의 발생가능성, 취약성, 영향을 평가하기 위한 방법론을 도출할 수 있었다.

〈표 1-4〉 정책협의회 및 전문가 자문 등

번호	구분	시기	기관	논의내용
1	정책협의회	’25.1.13.	해양경찰청 외사과	• 과제 방향 및 수행 방안의 적정성 자문 • 잠정 대응 방안의 현장성 및 적정성 자문 • 해양 복합위협 관련 데이터 협조 요청 • 해양 복합위협 관련 사례의 적정성 검토
2	전문가 자문회의	’25.1.16.	해양경찰청 정보과, 형사과	• 해양보안범죄 대응을 위한 해양경찰청 보안 체계 등에 관한 자문
3	전문가 자문회의	’25.2.21.	한국해양대학교 한국해양수산연수원 몽골 해사청	• 항만 등 연안지역 해양 치안 관리 제도 및 관련 법령 자문
4	전문가 자문회의	’25.2.25.	해양안보 및 항만보안 전문가	• 국내 항만보안 제도 배경 및 현황 관련 자문
5	전문가 세미나	’25.3.6.	위험성 평가 내부 전문가	• 국가관할해역 해양보안범죄 대응체계 취약성 및 영향분석을 위한 HVA 등 분석 방법론 세미나

번호	구분	시기	기관	논의내용
6	전문가 자문회의	’25.3.12.	해양경찰청 외사과 인천항보안공사	• 해양보안범죄 및 신흥 해양 복합위협 관련 동향 및 사례 자문 • 항만시설 해양보안범죄 및 신흥 해양 복합위협 대응체계 및 실태 관련 자문
7	전문가 자문회의	’25.3.20.	해양수산부 해운물류국	• 항만구역 해양 복합위협 대응체계 및 현황 관련 자문
8	전문가 자문회의	’25.4.9.	부산항만공사 보안과	• 부산항 보안 관리 현황 및 보안사고 대응체계 자문
9	전문가 자문회의	’25.4.10.	해양경찰청 외사과	• 해양 복합위협 사례 관련 자문
10	전문가 자문회의	’25.6.11.	한국해양대학교 해사인공지능보안학부	• 해양 복합위협 데이터 분석 및 GIS 핫스팟 분석 관련 자문
11	전문가 자문회의	’25.6.18.	한국해양대학교 국제무역경제학부	• 해양 복합위협 미래 위험성 평가 방법론 자문
12	전문가 자문회의	’25.7.16.	한국해양대학교 해사인공지능보안학부	• 2차 해양 복합위협 데이터 분석 및 GIS 핫스팟 분석 관련 자문
13	전문가 자문회의	’25.8.8.	해양경찰청 미래해양경비단, 외사과	• 국가관할해역 위협 감시체계 자문 • 해양 복합위협 위험성 평가 체계 자문
14	서면 자문 및 설문	’25.8.	관련 부처, 연구기관, 산하 기관 등 총 19개 기관 전문가 자문	• 해양 복합위협의 위험성 평가 설문 • 미래 해양 복합위협의 위험성과 국내 대응체계의 취약성에 관한 자문

자료: 저자 작성

제3절 선행연구 검토

1. 선행연구 분석

해양 복합위협에 관하여 포괄적인 정책을 중심으로 수행된 국내 선행연구는 많지 않다. 다만, 미국, 유럽 등을 중심으로 최근 변화하고 있는 테러

등 위협을 중심으로 분야별 경향을 분석한 보고서와 이에 대응하기 위한 협의의 제도 개선에 관한 연구는 다수 발견된다. 특히, 국내의 경우, 해양 국제범죄를 포함한 해양 복합위협에 관한 선행연구가 해양경찰청 등 특정 기관의 기능을 중심으로 관련 기관의 조직 및 역할을 강화하기 위한 정책 제언을 중심으로 수행되었던 것을 확인할 수 있다. 함혜현·전봉조·이장욱(2022)과 김재광(2019) 등 다수의 연구가 해양안전, 선박재난, 자율운항선박 등의 보안 개선을 위해 해양수산부, 해양경찰청 등 관련 부처의 기능 및 역할을 개선하기 위한 방안을 연구하고 있다. 일부 연구(박성수(2018), 유재두·노호래(2018), 정아신·양쥔·조정형(2024) 등)의 경우, 특정 해양 국제범죄(밀입국, 마약 등)에 대한 정책적 대응 방안을 제시하고, 이를 위해 공간 분석 기법을 활용하거나 사회적 비용 분석을 활용하고 있으나, 거시적 관점에서 해양 복합위협을 체계적으로 대응하기 위한 정책적 방안 제시에는 한계를 가지고 있다. 국외 연구의 경우, 범죄 정보에 대한 접근성 부족으로 국제범죄 자체에 관한 연구보다 거시적 관점을 중심으로 해양안보 정책, 위협 관리, 해양 외교에 관한 연구를 다수 확인할 수 있었다. 특히, Ringsberg & Cole(2020)의 경우 개별 국가의 항만보안 정책을 분석하여 정책적 시사점을 제공하고 있으며, 항만보안 정책이 해양 국제범죄 대응에 중요한 역할을 하고 있음을 강조하고 있다.

2. 선행연구와의 차별성

본 연구는 연구의 목표와 대상 및 범위, 방법 측면에서 선행연구와 차별성을 가진다. 먼저 연구 목표 측면에서 기존 연구가 전통적 위협에 효과적으로 대응하기 위한 관련 기관의 조직 개선, 인력 확보, 장비 개선 등에 중점을 두었다면, 본 연구는 해양 복합위협을 전통 및 미래 위협으로 구분하고, 일반 연안 및 항만구역으로 정책을 구분하여 관련 기관의 협력적 대응

체계 개선 방안 도출을 목표로 한다는 점에서 기존 선행연구와 차별성을 가진다.

또한 연구 대상 및 범위 측면에서 기존 연구가 주로 해양수산부 내지 해양경찰청 등에서 관리하는 주요 항만시설을 중심으로 관리 내지 경비 체계 등을 대상으로 연구가 이루어진 반면, 본 연구는 우리나라 관할 해역 및 위협 발생 지역을 중심으로 관련 기관들의 주요 역할 및 대응체계를 분석하고 해양 복합위협에 효과적으로 대응하기 위한 제도적 방안을 주요 대상으로 연구를 수행한다는 점에서 기존 연구와 차별성을 가진다.

마지막으로 연구 방법 측면에서 기존 연구가 문헌연구, 사례 분석, 설문조사, 비용 분석, 전문가 자문을 중점으로 연구를 수행했다면, 본 연구는 국내외 문헌을 비롯하여, 우리나라 해양 국제범죄 통계를 분석할 예정이며, 전문가 자문 외에도 위험성 평가, 정책 담당자와의 정책협의회, GIS 분석 등을 실시하여 위협의 발생 위치, 해상교통량, 관련 기관의 관할 범위 등과의 상관관계를 분석하여 위협에 대응하기 위한 지역별 효과적인 기관 간 협력체계를 도출한다는 점에서 연구 방법을 차별화했다.

〈표 1-5〉 선행연구와의 차별성

구분	선행연구		본 연구
	요약	참고문헌	
연구 목표	• 항만보안 제고를 위한 개선 방안 제시 • 밀수 및 밀입국 대응 방안 제시 • 해양보안범죄 등 해양위협 요인의 정보 수집에 관한 해양경찰 기능적 개선방안 제시 • MDA 체계 구축 방안 제시 • 일반적인 해양범죄 대응 방안 제시	• 함혜현·전봉조·이장욱(2022) • 박성수(2018) • 문경환(2017) • 김재광(2019) • 김영습 외(2021) • 이정훈 외(2020) • 박경규 외(2023) • 최정호(2016) • 유재두·노호래(2018)	• 밀입(출)국 및 밀수, 해양 사이버범죄, 해양보안범죄 등 해양 복합위협을 예방 및 대응하기 위한 기능적, 제도적, 정책적 개선 방안 제시

구분	선행연구		본 연구
	요약	참고문헌	
	• 연안지역 등의 범죄예방디자인 적용 제시	• Bichou, Szyliowicz, & Zamparini(2013)	
연구 대상	• 국가항만구역의 보안활동 관할권 • 연안여객선 보안위협 • 해상 밀수 및 밀입국 범죄 • 해양 정보활동 • 국가 MDA 체계 • 해양경찰 일반사법경찰권	• 김찬호·최건우·박상원(2017) • 주종광·이은방(2007) • 유재두·노호래(2018) • 김재운(2014) • 이순태·이유봉(2017) • 방호삼·하민재(2022) • 김희정(2022) • Gülcan & Erginer(2023) • UNODC(2013) • Larsson & Widen(2022) • Castaneda, Condit, & Wilson(2016)	• 해상을 통해 외부에서 유입되는 위협을 수반하는 범죄로 일반 해양범죄와 달리 국가 안보, 다중 인원에 대해 대량의 피해를 야기할 가능성이 큰 범죄 • 해양보안범죄를 예방, 대비, 대응하는 유관기관(해양수산부, 해양경찰청, 항만공사, 항만보안공사, 지자체 등)
연구 범위	• 연안여객선 대상 보안 위협 • 항만법상 항만구역 • 해운대 특정 지역 • 국가관할해역 • 인도·태평양 지역 • 스웨덴 항만 위협	• 백병선(2018) • 이정훈 외(2020) • 장윤석(2022) • Ringsberg & Cole(2020) • Fabris(2017)	• 해양보안범죄를 예방하는 기관의 정보활동, 대응 방안 및 수단 등 • 해양보안범죄에 대응하기 위한 우리나라 관할 해역 및 연안지역에 일반적으로 적용할 수 있는 법·제도
연구 방법	• 문헌연구 • KANO 모델 기반 CPTED • 비용 및 통계분석 • 설문조사 및 전문가 자문 • 정책 및 제도 비교 분석 • 사례연구	• 정아신·양쥔·조정형(2024) • 한재진·최정호(2020) • 함혜현(2022) • Fenton(2024) • UNODC(2019) • Deng et al.(2022)	• 문헌연구 • 통계분석 및 GIS 분석 • 취약성 분석(HVA, PEST) 및 FGI 분석 • 정책 및 제도 비교 분석 • 사례연구

자료: 저자 작성

02
해양 복합위협의 이론적 검토 및 주요 사례 분석

본 장은 연구의 대상인 해양 복합위협의 논의 동향을 분석하여, 분석의 대상 및 범위를 제시하고자 한다. 앞에서 언급한 바와 같이 해양 복합위협은 아직 법적으로 명확히 정의되거나 학문적으로 합의된 범위가 확립되어 있지 않다. 이에, 본 장에서는 최근 해양에서 발생하고 있는 국내외 해양위협에 대한 동향 및 경향을 문헌과 전문가 자문을 중심으로 분석하여 본 연구의 분석 대상을 도출하고, 해양 복합위협과 관련된 주요 사례를 분석하여 향후 국가적으로 대응해야 하는 해양 복합위협의 범위를 규명하고자 한다.

제1절 해양 복합위협 국내외 논의 동향

1. 해양 복합위협 국외 논의 동향

해양 복합위협은 사실상 해양이라는 공간에서 발생하거나 해양의 활동과

연계하여 발생하는 다양한 위협이 복합적인 공격 전달 수단 또는 공격 유형을 가지고 발생하는 것을 의미한다. 따라서 해양 복합위협의 논의 동향은 복합위협 논의의 한 분야로 살펴볼 수 있다.

현재 복합위협의 개념은 유럽을 중심으로 많은 논의가 이루어지고 있다. 특히, 유럽연합(EU: European Union) 집행위원회는 "EU 의회 및 이사회 공동 문서(Joint Communication to the European Parliament and the Council)를 통해 "복합위협 대응을 위한 공동 프레임워크(Joint Framework on countering hybrid threats)"에 대한 국가 단위의 논의를 본격화했다.[18] EU 집행위원회는 이 문서를 통해 복합위협이 다양하지만 변화하는 위협의 특성을 포괄하고 유연성 있게 대처하기 위해, 개념의 유연성을 유지하는 동시에, 국가나 비국가 행위자가 특정 목표를 달성하기 위해 외교적, 군사적, 경제적, 기술적 수단 등 전통 및 비전통적 방법을 혼합하여 강제적·파괴적 활동을 자행하는 것을 의미한다고 정의했다.[19]

1) 복합위협의 확대와 대응

특징적인 것은 이러한 복합위협이 네트워크 등 사이버를 매개로 주로 이루어지기 때문에, 물리적인 공격의 대상이 국경을 넘어 광범위하게 확대될 수 있다는 것이다.[20] 이에 EU 집행위원회는 회원국 및 동맹국 간 협력을 통해 복합위협을 포괄적으로 대응하는 것이 필요하며, 이를 위해 다국적 센터를 설립할 것을 제안하고 있다. 또한, EU 집행위원회는 복합위협이 국가의 취약점을 악의적으로 이용하고, 법치주의 및 민주주의 가치를 훼손하는 것을 주요 목적으로 하는 것을 강조하고, 국가별 취약점을 도출하기 위

18) European Commission(2016)(검색일: 2025.4.28.)
19) Ibid.
20) Ibid.

한 복합위협의 위험성 평가를 개발하여 도입하도록 추진하고 있다. 그리고 EU 집행위원회는 상황인식(Situational Awareness)을 통해 테러 자금 조달, 범죄행위자 모집 등에 관한 사이버 정보를 지속적으로 모니터링하고, 위협 정보의 흐름을 미연에 차단하고 정책적으로 대응하기 위한 보안 위험 평가 모델 또한 개발을 추진하고 있다.[21]

EU 집행위원회는 이러한 정책의 중심 역할을 담당하기 위해 2016년 공동 문서를 통해 유럽복합위협대응센터(Hybrid CoE: The European Centre of Excellence for Countering Hybrid Threats)를 설립하도록 제안했다.[22] 그리고 2017년 4월 11일 유럽복합위협대응센터는 9개국의 참여로 핀란드 헬싱키에 설립되었다. 2025년 현재 유럽복합위협대응센터 운영을 위해 총 36개국이 참여하고 있으며, EU 및 NATO 또한 전략 개발 및 교육 프로그램 운영을 위해 참여하고 있다.[23]

유럽복합위협대응센터의 주요기능은 현재까지 복합위협 대응 관련 전문 지식의 공급과 교육의 실시이며, 이를 통해 참여국의 안보를 강화하는 것을 궁극적인 목표로 하고 있다. 교육과 훈련을 위해 EU와 NATO가 참여하고 있으며, 지식 공급 등을 위해 정부, EU 및 NATO, 민간전문가, 학계 등 민간에서 군사에 이르기까지 다양한 분야의 전문가와 실무가가 참여하고 있다. 특히, 지식 공급과 관련하여 복합위협 사례 공유, 위협 대응을 위한 권고 등을 제공하고 있으며, 이는 참여국의 복합위협 예방 및 대응능력

21) Ibid.
22) Hybrid CoE, Establishment(검색일: 2025.4.28.)
23) 유럽복합위협대응센터의 최초 설립 참여국(9개국)은 핀란드, 스웨덴, 영국, 라트비아, 리투아니아, 폴란드, 프랑스, 독일, 미국이며, 이후 (2017) 에스토니아, 노르웨이, 스페인, (2018) 네덜란드, 이탈리아, 덴마크, 체코, 오스트리아, 캐나다, 루마니아, 사이프러스, (2019) 그리스, 헝가리, 룩셈부르크, 몬테네그로, 포르투갈, 슬로베니아, 튀르키예, (2020) 슬로바키아, (2021) 크로아티아, 벨기에, 아이슬란드, (2022) 몰타, (2023) 아일랜드, 불가리아, 북마케도니아, (2024) 알바니아 등 27개국이 추가로 참여하고 있음. 유럽복합위협대응센터 설립 및 목적에 관한 보다 상세한 사항은 European Commission (2016)(검색일: 2025.4.28.); Hybrid CoE, Establishment(검색일: 2025.4.28.); Hybrid CoE, Dates of accession for the Hybrid CoE, Participating States(검색일: 2025.4.28.) 참조

을 강화하는 데 중요한 역할을 담당하고 있다.[24]

2) 해양 복합위협 대응을 위한 협력

유럽복합위협대응센터는 설립 이래 해양 복합위협을 업무에 포함시켜서 관리하고 있다. 특히, 해양 복합위협의 효과적 관리를 위해 최근 해양 복합위협의 경향을 반영한 해양 인프라 보호에 관한 보고서(Protecting Maritime Infrastructure from hybrid threats: legal options)를 최근 발간했다.[25] 이 보고서는 최근 해양에서 발생하고 있는 복합위협의 특징과 보호 대상, 관련 제도 등을 제시하고 참여국이 이를 반영한 국내 정책들을 개발하도록 권고하고 있다. 이 보고서는 해양 복합위협을 별도로 정의하기보다 특정한 목적을 달성하기 위해 연안여객터미널, 항만시설, 시추시설, 해저케이블, 해양 관측 시설 등 주요 해양 인프라 시설에 대한 공격이 해양에서 발생하는 것을 해양 복합위협으로 정의한다.[26]

이 보고서는 주요 해양 인프라 시설에 대한 공격이 국가의 경제적, 사회적 피해뿐만 아니라, 막대한 해양환경 오염을 초래할 수 있다고 언급하고 해양 복합위협에 대응하기 위한 협력의 필요성을 강조한다.[27] 특히, 국경에 따라 대부분의 활동이 국내법에 따라 규율되는 육상과 달리 유럽의 경우, 해양은 주된 규범을 유엔해양법협약과 국제관습법으로 하고 있다. 즉, 육상은 국경을 기준으로 특정 활동에 대한 책임 소재가 상대적으로 명확한 반면, 해양에서는 하나의 행위에 대해 여러 국가의 의무와 책임이 혼재할 수 있으며, 이러한 행위를 규율하기 위해서는 다양한 법적 체계와 국가 시스템이 개입하게 된다는 것이다. 그리고 이러한 다양한 법적 체계와 여러

24) Hybrid CoE, What is Hybrid CoE(검색일: 2025.4.28.)
25) Sari(2025)
26) Ibid., p. 6.
27) Ibid., pp 6-7.

국가의 개입은 해양에서 복합위협이 발생했을 때, 다양한 국가기관의 협력을 요구하게 된다고 이 보고서는 강조한다.[28] 실례로, 과거 머스크 선사에 대한 2017년 NotPetya 악성 소프트웨어 공격, 2022년 노르트스트림 2(Nord Stream 2) 해저 관선 파괴, 선박자동식별시스템(AIS: Automatic Identification System) 정보의 위조, 2022년 및 2024년 해저 통신 케이블 절단 등은 해양 복합위협의 이러한 특징을 보여주는 대표적인 사건들이다.[29] 이들 사건은 주로 특정 경제적·정치적 목적을 달성하기 위해 연안에 위치한 해운회사를 공격하거나 해양의 주요 인프라 시설을 손상시켰던 사례들로서 하나의 국가를 넘어 유럽지역에 많은 경제적 피해를 입혔던 사건들이다.

2. 해양 복합위협 국내 논의 동향

해양 복합위협에 관한 국내의 최근 논의는 최근 급속한 기술 발전으로 군사적, 비군사적 요소가 중첩되어 한층 복잡화되는 경향을 보이는 최근 사례를 중심으로 국가 차원의 해양위협의 감시와 관리, 거버넌스 구축의 필요성을 중심으로 이루어지고 있다.[30] 다만, 국내는 유럽과 같이 복합위협을 전문적으로 관리하는 단일 기관을 설립하기보다, 정책, 치안, 안보, 과학기술 등 각 분야에 따라 여러 기관이 각자의 역할과 특성에 따라 복합위협을 연구하고 관리하는 방식으로 접근하고 있다. 이에 분야별 해양 복합위협에 관한 논의 동향을 살펴보면 다음과 같다.

28) Ibid., p. 7.
29) 개별 사건에 대한 보다 상세한 내용은 목록별로 다음의 자료 참조. CNBC(2017.8.16.)(검색일: 2025.4.28.); Stensrud & Østhangen(2024); Østhangen(2023); DW(2023.9.25.)(검색일: 2025.4.28.); Foreign Policy(2024.12.4.)(검색일: 2025.4.28.); Reuters(2025.2.22.)(검색일: 2025.4.28.)
30) 구체적인 사례는 본 장 제3절 해양 복합위협 주요 사례 분석 참조.

먼저, 정책 연구기관을 중심으로는 외교 및 안보적 관점에서 국가 중요 기반시설 위협 및 국가 행위자로 인한 관할 해역 위협 등에 대응하기 위한 정책 수단 개발이 최근 주로 논의되고 있다. 특히, 정책 연구기관들은 최근 대만 해협, 발트해 등지에서 발생한 해저케이블 손상 내지 절단 사건을 중심으로 국가 주요 해양시설에 대한 위협이 가져올 수 있는 국가 기능 마비 상황 등을 분석하여 이러한 위협에 대응하기 위해 국제 수사 공조 내지 다자협력과 범부처 협력체계를 구축해야 할 것을 강조하고 있다.[31] 또한, 정책 연구기관들은 최근 우리나라 주변의 관할권 중첩해역에서 발생하고 있는 외국선박의 불법조업 활동과 양식 시설물 설치 등이 우리나라 해양 영토 주권과 안보에 부정적 영향을 미칠 수 있음을 주목하고 이에 대응하기 위해 범정부 차원의 다양한 정책적 방안들이 개발되어야 함을 논의하고 있다.[32]

다음으로 과학기술 연구기관과 안보 기관을 중심으로는 사이버안보, 무인체계를 활용한 위협 등에 대한 논의가 다양하게 이루어지고 있다. 특히, 국제해사기구(IMO, International Maritime Organization)는 2032년까지 자율운항선박을 상용화하기 위한 구속력 있는 국제기준을 개발하기 위해 계획을 수립하고 추진하고 있어, 관련 연구기관과 안보 기관은 자율운항선박의 안정적 운용을 위한 해상 사이버보안 기술과 관련 기준 개발에 대한 논의를 활발하게 진행 중이다.[33] 이와 더불어, 국방과학연구소 등 안보 기관을 중심으로 최근 러시아-우크라이나 전쟁 및 이스라엘-이란 전쟁에서 등장했던 군집 무인수상정 등 해상 무인체계를 활용한 주요 항만시설 및 해상교량 파괴, 유조선 공격 등을 대비하기 위한 기술 개발 논의 또한 활발하게 이루어지고 있다.[34]

31) 신소현·임정희(2025), pp. 13-14; 정현욱·김소정(2025), p. 7; 반길주(2025A), p. 178 등 참조
32) 반길주(2025B); 정현욱(2025); 이서항(2023); 해양경찰청 보도자료(2024.4.30.)(검색일: 2025. 9.6.) 등 참조
33) Korea Shipping Gazette(2024.12.31.)(검색일: 2025.9.6.)
34) 류재학·허지용·나윤후(2023); 연합뉴스(2025.6.17.)(검색일: 2025.9.6.); 연합뉴스(2022.9.15.)(검색일: 2025.9.6.) 특히, 무인체계와 관련하여 국방과학연구소 및 해군을 중심으로 다양한 기술 발전

마지막으로, 해양 복합위협에 대한 정부기관의 논의 또한 활발하다. 정부기관들의 주요 논의는 정책 연구기관과 유사하게, 해양 주요 인프라에 대한 위협과 관할 해역 해양 주권 보호 등을 중심으로 이루어지고 있다.[35] 다만, 이들 논의는 국익을 보호하기 위한 국가 기능을 효율적으로 실현하기 위해 복합위협을 실질적으로 대응하기 위한 방안 모색, 국가 간 협력체계 구축 등을 중심으로 이루어지고 있다.

예를 들어 외교부는 신흥 안보 위협에 대응하기 위한 국제사회 논의를 주도하기 위해 '세계신안보포럼(WESF: World Emerging Security Forum)'을 개최하고 있으며, 가장 최근인 2024년에는 스톡홀름국제평화연구소(SIPRI: Stockholm Interantioanl Peace Research Institute)와 한국과학기술원(KAIST: Korea Advanced Institute of Science and Technology)과 함께 '진화하는 안보 환경 속 국제협력 – 사이버, AI, 신기술을 중심으로'라는 주제로 포럼을 개최했다.[36] 특히, 이 포럼에서 사이버 안보는 단순 침해와 피해를 넘어 핵심기반시설 공격을 통해 국제 평화와 안보에 막대한 영향을 미칠 수 있다고 강조하고 이에 대응하기 위한 다자주의 국제규범 형성 및 이행, 역량강화를 위한 국제협력 등이 강조되었다.[37]

외교부는 2025년에도 세계신안보포럼을 '하이브리드 위협의 진화와 국제안보(The Evolution of Hybrid Threats and international Security)'를 주제로 진행되었다. 본 포럼에서 외교부는 인지전, 신흥기술로 인한 전쟁 양상의 변화, 핵심인프라 공격 등 우리 사회가 다양한 형태의 하이브리드 위협에 직면해 있다고 밝히며, 이러한 위협을 대응하기 위해 △사회적 연대의 중요성, △회복력 강화, △신기술의 국제법과 국제규범에 따른 발전

세미나가 개최되고 있음

35) 해양수산부 보도자료(2025.5.1.)(검색일: 2025.9.7.); 외교부(2024.12.6.)(검색일: 2025.9.6.) 등 참조.

36) 외교부(2024.12.6.)(검색일: 2025.9.6.)

37) 외교부(2024.12.6.)(검색일: 2025.9.6.)

과 책임있는 사용, △정부와 민간 협력의 중요성을 강조했다.[38] 이와 더불어, 한국과학기술원(KAIST) 이광형 총장은 하이브리드 위협이 국가의 핵심 기능과 민주적 가치를 위협하고 있으며, 이를 대응하기 위해서는 △정책적 통찰력, △전략적 안보 이해, △긴밀한 국제적 공조가 필수적이라고 강조했다.[39] 특히, 본 포럼에 참석한 스톡홀름국제평화연구소(SIPRI)의 카림 하가그(Karim Haggag) 소장은 하이브리드 위협의 다면적 성격과 특징을 설명하고 군사·정치·사회·기술 등 다양한 영역을 포괄한 총체적인 대응의 중요성을 강조했다. 외교부는 본 포럼에 앞서 사전 준비의 일환으로 지난 7월 '하이브리드 위협의 진화와 국제안보'를 주제로 국내 전문가를 중심으로 포럼을 개최하기도 했다.[40] 이 포럼에서 참석자들은 하이브리드 위협이 사이버, 인공지능, 드론 등 신기술 발전에 따라 그 영향이 확대되고 있음을 강조하고 이에 대응하기 위한 국가적인 방향을 보다 구체적으로 수립할 수 있도록 위협의 정도를 지표화는 등의 체계적인 준비가 필요함을 논의했다.[41]

해양수산부의 경우, 과거부터 해적 및 테러 등 해양에서 발생할 수 있는 물리적 위협을 중심으로 대응 방안을 지속적으로 논의해 오고 있으며, 최근에는 자율운항선박, 스마트항만 등을 중심으로 사이버위협에 대응하기 위한 제도적 방안과 범부처 협의 사항에 대해 논의하고 있다. 해양 복합위협 중 전통적이면서 물리적 위협과 관련하여 해양수산부는 2005년부터 해적 및 선박 보안 세미나를 개최하고 있으며, 이를 통해 관련 업계와 정부의 해적, 테러 등 선박 보안 대응역량 강화를 도모하고 있다.[42]

가장 최근 개최된 2024년 10월 해적 및 선박 보안 세미나는 국내외 테

38) 외교부 보도자료(2025.9.8.)(검색일: 2025.10.31.)
39) 외교부 보도자료(2025.9.8.)(검색일: 2025.10.31.)
40) 외교부 보도자료(2025.9.8.)(검색일: 2025.10.31.)
41) 외교부(2025.7.14.)(검색일: 2025.9.6.)
42) 해양수산부 보도자료(2024.10.30.)(검색일: 2025.9.7.)

러 정세, 해적 동향과 최근 확인되고 있는 선박 보안관리 취약 요인 및 개선 방안에 대해 논의하였으며, 최근 중동분쟁에 따른 민간 선박 피해사례 공유, 우리 선박 위급 상황 시 대응 요령 등을 설명하고 아덴만에서 작전 중인 청해부대의 협조 사항을 공유했다.[43] 해적 및 선박 보안 세미나에는 외교부, 해군, 기타 보안기관 등 또한 참여하여 해양위협에 대해 논의하고 있다. 특히, 외교부는 유엔안전보장이사회 대북 제재 결의 중 불법 해상 환적, 신규·중고 선박 반입 제한에 관한 사항에 대해 논의하고 우리나라 국적 해운 선사와 관련 업체가 북한의 제재 회피 행위에 의도치 않게 연루되지 않도록 유의사항을 공유했다.[44]

또한 해양수산부는 2025년 4월 28일부터 30일까지 제10차 아워오션콘퍼런스(Our Ocean Conference)를 국내에 유치하여 개최하였으며, 콘퍼런스 주요 주제 중 하나를 '해양안보'로 의제하고 전 세계 공급망의 중심축인 해양의 안정적 질서 유지를 위한 협력 방안에 대해 논의했다.[45] 구체적으로는 해상교통로 보호, 해적 및 불법조업 대응, 해저케이블 손상 방지, 해양안보 거버넌스 강화 등의 사안이 주요 의제로 논의되었다.[46]

해양수산부는 해양 복합위협과 관련하여 주요 쟁점이 되고 있는 사이버위협에 대해서도 2022년부터 해사 사이버안전 전문가 토론회를 통해 논의하고 있다. 해사 사이버안전 전문가 토론회는 미래 자율운항선박 등 차세대 선박의 확산과 관련하여 사이버위협으로 인한 해양안전 및 테러 문제를 논의하기 위해 2022년 구성되었다.[47] 2025년에는 토론회의 명칭을 해사 사이버안전 전문가 포럼으로 변경하고, 2025년 6월 포럼을 개최하여 최근

43) 해양수산부 보도자료(2024.10.30.)(검색일: 2025.9.7.)
44) 위의 자료; 해양수산부 보도자료(2023.11.28.)(검색일: 2025.9.7.); 해양수산부 보도자료(2022.11.28.)(검색일: 2025.9.7.)
45) 해양수산부 보도자료(2025.5.1.)(검색일: 2025.9.7.)
46) 위의 자료
47) 해양수산부 보도자료(2022.11.24.)(검색일: 2025.9.7.)

해사 분야 사이버 공격 사례를 공유하고, 이에 대한 효과적인 대응 방안을 논의하는 한편 초고속 해상 통신망 등이 선박의 운항 시스템에 미치는 영향과 사이버 공격 취약성 등에 대해서도 논의하였다.[48]

이러한 논의와 더불어, 해양수산부는 해양 사이버 공격 및 침해에 제도적으로 대응하기 위해 지난 2024년 10월 "해사 사이버안전 관리 강화방안"을 관계부처와 합동으로 발표하였다.[49] 이 방안은 선박 장비 및 기자재 등을 중심으로 선박-육상 간 네트워크 연결성이 확대되어, 육상 및 해상 시스템의 보안시스템에 사이버 취약점이 새롭게 등장하는 것을 고려하여, 이들에 대한 사이버위협과 공격을 관리하기 위해 수립되었다.

선박 장비 및 기자재와 항만 및 선사의 네트워크 연결성 확대는 선박, 해운사, 항만의 운영시스템이 사이버 공격에 노출되는 빈도를 확대한다. 실제 국외에서는 선사·선박 운항시스템을 무력화하고 원격 조정 등을 통해 선박을 나포하거나 금전을 요구하는 등의 사이버 공격 사례가 발생한 적도 있다.[50] 이에 해양수산부를 중심으로 관련 기관들은 △ 선사·선박·항만의 사이버안전 관리 체계를 수립하기 위한 민간 대응 역량 강화, △ 선사·선박·항만의 사이버안전 관리 체계를 구축 및 이행하는 거버넌스 구축, △ 선박 장비 및 항만 등에 대한 사이버 공격 위협 요인을 탐지·대응하는 기술 개발 등을 정책 추진 방안으로 이 강화방안을 통해 제시하고 있다.[51]

해양수산부의 해양 복합위협에 대한 이러한 정책적 접근과 더불어 해양경찰청 또한 해양 복합위협과 관련하여 감시체계 고도화, 현장 대책 및 대

48) 해양수산부 보도자료(2025.6.23.)(검색일: 2025.9.7.); 해양한국(2025.7.28.)(검색일: 2025.9.7.)
49) 해양수산부 보도자료(2024.10.31.)(검색일: 2025.9.7.); 대한민국 정책브리핑(2024.10.31.)(검색일: 2025.9.7.)
50) 해양수산부 보도자료(2024.10.31.)(검색일: 2025.9.7.) 이 보도자료에서는 선박 대상 사이버 공격으로 운항통제권을 10시간 상실한 사례, 선사 시스템이 랜섬웨어에 감염되어 약 3천억 원의 손해를 입은 사례 등이 해외에서 보고되고 있다고 밝히고 있다.
51) 해양수산부 보도자료(2024.10.31.)(검색일: 2025.9.7.); 대한민국 정책브리핑(2024.10.31.)(검색일: 2025.9.7.)

응 역량 강화, 위협 대응을 위한 현장 기술 개발 등과 관련하여 다양한 논의와 연구를 수행하고 있다. 특히, 해양경찰청은 미래 해양경비체계 발전을 위한 정책 공개 토론회를 2025년 9월 3일 국회에서 개최하고 이를 통해 △ 해상 법집행력 강화를 위한 「해양경비법」 고도화, △ 해양력 강화를 위한 K-MDA 체계 발전방안 등에 대해 논의했다.[52] 이를 통해, 해양경찰청은 불법조업, 외국선박의 우리 관할 해역 침범 등 우리나라 관할 해역에서의 물리적 위협에 대응하기 위한 법집행력 강화 입법 방안을 논의하였고, 더불어 다양한 해양의 위협 요소를 광역 감시 자산으로 원거리까지 탐지하고, 국내외 분산된 선박신호와 해양 빅데이터를 융합하여 분석·활용하는 MDA 체계 구축에 대해서도 논의했다.[53]

제2절 해양 복합위협의 정의 및 범위

1. 해양 복합위협의 개념과 정의

해양 복합위협에 관한 국내외 논의 동향을 고려할 때, 4차 산업혁명 및 무인기술의 상용화로 해양위협의 대상과 형태가 확대되고 있어 이에 대응하기 위한 다양한 정책적 수단이 필요한 것으로 판단된다. 과거 위협의 대상은 정치, 경제, 이념 목적을 달성하기 위한 군사적 침해, 해적, 불법조업 등 물리적 위협에 한정되었다. 그리고 이러한 물리적 위협은 상당한 기술과 자본 등이 요구되어 실질적인 위협의 실현에 한계가 있었으며, 위협 행위에 가담한 인원 또한 비밀 유지 등으로 제한적이었다. 그러나 최근 4차

52) 해양경찰청 보도자료(2025.9.3.)(검색일: 2025.9.7.)
53) 위의 자료

산업혁명에 따른 사이버 수단의 대중화는 외로운 늑대 등 개인이 불특정 다수를 대상으로 위협 행위를 쉽게 저지를 수 있는 환경을 제공하고 있을 뿐만 아니라, 개인이 타인의 위협 행위에 전 세계에서 은밀하게 가담할 수 있는 환경 또한 제공하고 있다.[54]

결국 해양 복합위협의 대상은 기존의 군사적·경제적 위험뿐 아니라 첨단 기술 적용으로 인한 사이버 공격, 자율운항선박 관련 사고 및 테러의 활용, 해상 물류 공급망 교란 등 다양한 새로운 위험으로 확대하고 있다. 특히, 전통적 해양테러, 해적, 불법조업, 밀수뿐만 아니라 전파 교란, 선박·항만 ICT 시스템 해킹, 스마트 항만 설비 무력화 같은 디지털 기반 복합위협은 해상 물류와 경제 안보, 해양주권에 직접적인 영향을 미치며, 피해 확산 속도와 복잡성 면에서도 과거와 달리 치명적인 결과를 초래하는 특징을 보인다.[55] 이에, 이러한 위협에 대응하기 위해서 국내적으로 범정부 차원의 관리 방안 내지 통합적 관리 수단의 필요성을 주요 연구 및 정부기관이 언급하고 있으며, 이를 통해 해양 복합위협의 효과적 대응을 위한 국가 간 협력 체계 또한 구축하는 것이 필요함을 강조하고 있다.

해양 복합위협의 국내외 논의 동향을 분석할 때, 본 연구에서 분석하고자 하는 '해양 복합위협(Maritime Hybrid Threats)'은 해양을 통해 또는 해양에서 발생하는, 혹은 해양과 연계하여 발생하는 복합위협으로 정의할 수 있다. 해양에서 발생하는 위협 중 외부의 요인으로 국가 안보, 국익, 국민의 삶에 영향을 미칠 수 있는 위협을 말한다.

복합위협(Hybrid Threats)은 일반적으로 지상, 해상, 사이버 공간에서

54) 신용도·조홍제(2018), p. 58; 윤봉한·이상진·임종인(2015), pp. 133-134. 이들 연구는 인터넷 등 사이버 공간이 개인의 테러 또는 위협의 가담, 활동 준비에 상당한 도움을 제공할 수 있으며, 이로 인해 외로운 늑대 등과 같은 단독 테러 증가에 사이버 수단이 기여하고 있다고 분석하고 있다. 특히 인터넷은 테러 행위자에게 강력한 선전수단임과 동시에 보안성이 뛰어난 공간이며, 저비용 고효율성의 활동 환경을 제공하고, 위협 대상에 은밀히 접근할 수 있도록 정보를 제공하며, 무기 등 공격 수단을 쉽고 은밀하게 구할 수 있는 경로로 분석함

55) 최근 해양 복합위협 사례는 본 장의 해양 복합위협 주요 사례 분석 참조.

다양한 공격 형태를 가지고 “전통적인 군사적 공격과 비군사적 수단을 결합하여 특정 국가나 비국가 행위자를 압박하고 혼란을 일으키는 복합적인 위협”을 말한다.[56] 특히, 연구기관을 중심으로 2020년 이후 진행된 복합위협 동향, 정의, 국가 대응 전략 필요성 등에 대해 살펴보면. 무기 등 물리적 수단과 사이버 등 비물리적 수단을 혼합하여 국가나 비국가 행위자를 압박하고 혼란을 일으키는 복합적인 위협을 복합위협(‘하이브리드 위협’ 등으로도 표시)으로 정의하고 있다.[57]

〈표 2-1〉 복합위협과 해양 복합위협 정의

구분	내용
복합위협	• 대규모의 군사력을 사용하지 않고, 공격 주체의 노출을 최소화하며, 공격의도를 은폐하면서 전략적 목적을 달성하려는 ‘무정형 전략(amorphous strategy)’ • 전통적인 군사적 공격과 비군사적 수단(예: 사이버 공격, 경제적 강압, 정보전 등)을 결합하여 특정 국가나 비국가 행위자를 압박하고 혼란을 일으키는 복합적인 위협
해양 복합위협	• 해양을 통해 또는 해양에서 발생하는, 혹은 해양과 연계하여 발생하는 복합위협 • 국가나 비국가 행위자를 압박하고 혼란을 일으키기 위해 물리적 수단과 비물리적 수단을 혼합하여 해양에서 발생하는 복합적인 위협

자료: 송태은(2020), p. 6; 김소정(2024), p. 2를 참조하여 저자 작성

따라서 해양 복합위협은 국가나 비국가 행위자를 압박하고 혼란을 일으키기 위해 물리적 수단과 비물리적 수단을 혼합하여 해양에서 발생하는 복합적인 위협으로 정의할 수 있다. 특히, 해양 복합위협이 해양에서 발생하는 복합위협으로 무기 등 물리적 수단과 사이버 등 비물리적 수단을 혼합하여 국가나 비국가 행위자를 압박하고 혼란을 일으킨다는 점을 고려할 때,

56) 송태은(2020), pp. 1-2; Hybrid CoE, Hybrid threats as concepts(검색일: 2025.4.28.); 김소정(2024), p. 2.

57) 송태은, 앞의 보고서, p. 6; 김소정, 앞의 보고서, p. 2. 송태은의 연구에서 복합위협의 특징은 “직접 군사력을 사용하는 ‘하드파워(hard power)’와 여론에 영향을 끼치고 사회분열을 촉발하는 정치적 심리전 등 ‘소프트파워(soft power)’ 혹은 ‘샤프파워(sharp power)’ 수단을 다양하게 혼합하여 사용하는 것”이다. 김소정의 연구는 “이러한 위협의 목적은 대상 사회를 불안정하게 만들고, 정부의 의사결정을 방해하며, 국가의 회복력을 약화”시키는 데 있음을 강조

해양 복합위협은 해양 국제범죄, 해양테러, 해양 사이버위협이 주된 유형이라 할 수 있다.

2. 해양 복합위협의 범위와 유형

우리나라는 국내적으로 범정부 또는 국가 차원에서 해양 복합위협을 특별히 구분하여 대응하고 있지는 않다. 따라서 유럽 등 주요 선진국에서 지역 및 국가적 차원에서 관리 및 대응하고 있는 해양 복합위협을 우리나라는 개별 부처를 중심으로 관리 및 대응하고 있다. 다만, 해양테러, 밀수, 밀입국 등 일부 특정 해양 복합위협의 경우, 관련 부처 내지 기관 간 협력체계를 구축하고 있으나, 책임성 있는 제도를 통한 효과적 협력보다 기관 간 역할을 강조하는 병렬적 협력체계를 주로 구축하고 있다.[58] 그럼에도 불구하고 국내 제도에서 정의하고 있는 개별 행위를 근거로 해양 복합위협의 범위를 분석하면 다음과 같다.

1) 해양 복합위협의 범위

(1) 해양 국제범죄

해양 국제범죄는 해양에서 발생하는 국제범죄(transnational crimes)로서 "2개국 이상 또는 1개국에서 실행되었으나 그 과정의 중요한 부분이 다른 국가와 관련되거나 다른 국가에 효과를 미치는 중대범죄로서, 사회적으로 많은 영향을 미치는 범죄를 의미한다.[59] 이러한 개념은 국제범죄를 실무상 다루기 위해 구분하고 있는 것으로 법 또는 권한 있는 기관의 해석을 통해 정의된 것은 아니다. 이는 국제범죄를 하나의 통일된 형태로 정의하

58) 보다 상세한 사항은 제4장 제1절 해양 복합위협 국내 대응체계 분석 참조.
59) 국가정보원, 국제범죄(검색일: 2025.4.28.)

기에 범죄의 형태가 다양할 뿐만 아니라, 범죄의 귀속, 행위자의 처벌, 피해자 구제, 범죄 수사 및 처리 절차, 실체적 정의 및 구성 요건, 관할권 등과 관련된 다양한 문제들이 존재하기 때문이다.[60]

다만, 초국가적 범죄라고 지칭되는 국제범죄는 「국제연합 초국가적 조직범죄 방지협약」에서 그 주된 범위를 확인할 수 있는데, 이 협약 제3조는 초국가 범죄(transnational crimes)를 "조직범죄단체에의 참여"(제5조), "범죄수익 세탁"(제6조), "사법방해"(제23조) "범죄가 성질상 초국가적이고 조직범죄단체가 관여된 중대범죄"(제2~3조)로 정하고 있다. 그리고 이 협약은 "중대범죄"의 범위를 "법정형이 장기 4년 이상의 자유형 또는 이보다 중한 형벌로 처벌할 수 있는 범죄를 구성하는 행위"로 정하면서,[61] 같은 조에서 초국가의 요건을 △ 1개국 이상의 국가에서 범하여지는 경우, △ 1개국에서 범하여지나 그 준비, 계획, 지시 또는 통제의 중요한 부분이 다른 국가에서 수행되는 경우, △ 1개국에서 범하여지나 1개국 이상의 국가에서 범죄행위에 가담한 조직범죄단체가 관여된 것인 경우, △ 1개국에서 범하여지나 다른 국가에서 중요한 효과를 갖는 경우로 정하고 있다. 사실상 두 개 이상의 국가에 영향을 미치는 범죄 형태를 대부분 포괄하나, 4년 이상의 자유형이 적용되는 중대범죄로 한정하고 있어 이를 국제범죄의 보편적 의미로 해석하기는 어렵다.[62]

사실 국제범죄는 통상적으로 국제형사법의 규율을 받는 범죄를 국제범죄(international crimes)로 지칭하는데, 이러한 범죄는 집단살해죄, 인도에 반한 죄, 전쟁범죄, 침략범죄를 의미한다.[63] 그러나 이러한 범죄는 통상적으로 국제형사재판소의 규정에 따라 소추 절차가 이루어지고 유엔을 중심으로 별도의 국제법적 대응체계가 이루어져 있어 복합위협의 범주에는 포

60) 박주상·박동균(2010), pp. 67-68; 이종화(2003), pp. 195-196.
61) 국제연합 초국가적 조직범죄 방지협약 제3조 제1항
62) 국제연합 초국가적 조직범죄 방지협약 제3조 제2항
63) 국제형사재판소에 관한 로마규정 제5조

함할 수 있으나 본 연구의 목적을 위해 적용할 수 있는 국제범죄라고는 할 수 없다.

실제로, 국제범죄의 정의 및 유형에 대한 논의는 상당히 다양하다. 국가정보원 등에서 참고하는 「국제연합 초국가적 조직범죄 방지협약」상의 국제범죄는 초국가적 조직범죄를 효과적으로 예방하고 퇴치한다는 협약의 목적[64]을 달성하기 위해 국가 간 합의된 국제범죄에만 적용되는 것으로 이러한 정의를 보편적 의미에서 국제범죄로 적용하기는 어렵다. 게다가 전통적으로 형사사법은 국가의 고유권한이며 주권의 일부로 인식되어 오고 있어, 「국제연합 초국가적 조직범죄 방지협약」의 대상 범죄가 아니라도 일국의 관할하의 형사사법체계의 적용을 받으면서 2개국 이상의 국제공조를 필요로 하거나 타국과의 이해관계를 가진다면, 이는 그 나라 제도하에 국제범죄로 처벌받을 수 있다.[65]

이에 본 연구에서는 국내법상 우리 관할 해역에서 관련 기관의 규율 대상이 되는 국제범죄를 해양 국제범죄의 범위로 정한다. 특히 이러한 범죄에는 「국제항해선박 및 항만시설의 보안에 관한 법률」(약칭: 국제선박항만보안법)상 항만시설이나 항만 내의 선박에 위법하게 위해물품을 반입·은닉하는 행위,[66] 「출입국관리법」, 「밀항단속법」 등을 위반하여 해상을 통해 밀입(출)국을 하는 행위, 「관세법」, 「야생생물법」, 「마약류관리법」(약칭: 마약류관리법), 「검역법」 등을 위반하여 마약 등 신고되지 않은 물품을 불법적으로 국내로 유입하거나 외부로 유출하는 행위, 「형법」상 선박에서 타국인에게 행하는 폭행 등이 포함된다.

(2) 해양테러

64) 국제연합 초국가적 조직범죄 방지협약 제1조
65) 채성준(2016), pp. 298-299.
66) 국제선박항만보안법 제33조 제1항, 제47조 참조

해양테러와 관련하여 「국민보호와 공공안전을 위한 테러방지법」(약칭: 테러방지법) 제1호는 테러의 개념을 "국가·지방자치단체 또는 외국 정부의 권한행사를 방해하거나 의무 없는 일을 하게 할 목적 또는 공중을 협박할 목적으로 하는 행위"로 정의하며, 그중 해양에서 발생하는 테러의 범위를 선박 또는 해상구조물과 관련된 위해 행위, 선박 또는 해상구조물을 강탈하거나 운항을 강제하는 행위, 선박의 안전을 위태롭게 하기 위하여 선박의 기기·시설을 파괴하거나 손상을 가하는 행위 등으로 정하고 있다.[67]

(3) 해양 사이버위협

해양 사이버위협은 본 연구의 목적상 단순한 침해행위를 벗어나 정치·이념·종교적 동기를 지니고 정보시스템, 네트워크, 데이터를 공격하여 사회적 혼란을 야기하거나 특정 목표를 달성하려는 행위를 말한다고 할 수 있다. 국가정보원의 「사이버안보 업무규정」은 "사이버 공격·위협"을 "해킹, 컴퓨터 바이러스, 서비스거부(DDos: Distributed Denial of Service), 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협"으로 정하고 있다. 이러한 정의에 따라 국가정보원은 사이버위협을 사이버 범죄와 사이버 테러리즘으로 분류하여 관리하고 있다.

67) 테러방지법 제1호 다목
다. 선박(선박 및 해상구조물에 대한 위해행위의 처벌 등에 관한 법률(약칭: 선박위해처벌법) 제2조 제1호 본문의 선박을 말한다. 이하 이 목에서 같다) 또는 해상구조물(같은 법 제2조 제5호의 해상구조물을 말한다. 이하 이 목에서 같다)과 관련된 다음 각각의 어느 하나에 해당하는 행위
1) 운항(같은 법 제2조 제2호의 운항을 말한다. 이하 이 목에서 같다) 중인 선박 또는 해상구조물을 파괴하거나, 그 안전을 위태롭게 할 만한 정도의 손상을 가하는 행위(운항 중인 선박이나 해상구조물에 실려 있는 화물에 손상을 가하는 행위를 포함한다)
2) 폭행이나 협박, 그 밖의 방법으로 운항 중인 선박 또는 해상구조물을 강탈하거나 선박의 운항을 강제하는 행위
3) 운항 중인 선박의 안전을 위태롭게 하기 위하여 그 선박 운항과 관련된 기기·시설을 파괴하거나 중대한 손상을 가하거나 기능장애 상태를 일으키는 행위

〈표 2-2〉 사이버위협의 종류

구분	내용
사이버 범죄	• 사이버 공간을 이용한 불법행위나 사이버 공간에서 획득한 정보의 이용 과정에서 발생하는 각종 범죄로 정보통신망을 매개한 경우와 매개하지 않은 경우가 있다.
사이버 테러리즘	• 공격의 주체가 테러리스트, 테러집단, 국가행위자 등으로 컴퓨터 또는 컴퓨터 통신망을 통해 정부 혹은 민간 기관의 정보시스템에 침입하여 중대한 장애를 발생시키거나 파괴하는 등의 범죄행위 또는 폭력적 상황을 유발시킬 목적으로 무차별적 대상을 목표로 인터넷을 활용, 사이버 공격을 가하는 것을 말한다.

자료: 국가정보원, 사이버범죄(검색일: 2025.4.28.); 국가정보원, 사이버 테러리즘(검색일: 2025.4.28.) 참조하여 저자 작성

국가정보원은 사이버범죄의 유형을 또한 정보통신망 침해 범죄, 정보통신망 이용 범죄, 불법콘텐츠형 범죄 세 가지로 구분하고 있으며, 그 내용은 〈표 2-3〉과 같다.

〈표 2-3〉 사이버 범죄의 유형

구분	내용	종류
정보통신망 침해 범죄	• 정당한 접근권한 없이 또는 허용된 권한을 초과하여 컴퓨터나 정보통신망에 침입해 시스템, 데이터 등을 훼손, 멸실, 위·변조하고 정보통신망에 장애를 발생하게 하는 범죄	• 해킹, 서비스거부(DDoS), 악성프로그램, 기타 정보통신망 침해형 범죄
정보통신망 이용 범죄	• 범죄의 핵심 구성 요건에 해당하는 행위를 정보통신망에 이용하거나 이를 통해 실행하는 범죄	• 사이버 사기, 사이버금융사기, 개인·위치정보 침해, 사이버 저작권 침해, 사이버스팸메일, 기타 정보통신망 이용형 범죄
불법콘텐츠형 범죄	• 정보통신망을 통해 불법정보를(음란물, 불법 도박물, 불법콘텐츠 등) 배포, 거래, 임대, 전시하는 등의 범죄	• 사이버성폭력, 사이버도박, 사이버 명예훼손·모욕, 사이버스토킹, 기타 불법콘텐츠 범죄, 사이버스팸메일

자료: 국가정보원, 사이버범죄(검색일: 2025.4.28.)를 참조하여 저자 작성

실제로 사이버범죄는 그 자체로 완결된 범죄행위로서 복합위협의 형태로 나타나기보다 그 자체가 결과적인 행위가 된다. 반면, 사이버 테러리즘의 경우 인터넷을 활용하여 물리적인 범죄행위 또는 폭력적 상황을 유발하기

도 한다. 이에 국가정보원은 사이버 테러리즘의 구체적인 유형을 〈표 2-4〉와 같이 분류하여 관리하고 있다.

〈표 2-4〉 사이버 테러리즘의 유형

구분	내용	사례
기반시설 공격	• 하드웨어, 운영 플랫폼, 컴퓨터 관련 프로그래밍 파괴나 와해	• 랜섬웨어, 트로이목마, 웜, 스파이웨어, 로그웨어, 파일리스 맬웨어, 바이러스, APT(지능형 지속 공격), 공급망 공격, 개발자의 CI/CD 인프라 공격, 소셜 엔지니어링을 통한 악성코드 투하, 디도스 공격, 피싱, 스피어피싱, 보이스피싱, 스푸핑, 스키밍, 워터링 홀, 드라이브 바이 다운로드, 다크웹, 스캠, 파밍, 메모리해킹, 스파이앱, 몸캠피싱
정보시스템 공격	• 특정 시스템에 저장된 정보를 손상, 파괴, 변조하는 것	
기술적 조장	• 테러사건을 지원하기 위해 사이버·디지털 기술을 사용하거나 테러 공격을 조정·선동하는 것	
홍보·기금마련	• 테러조직의 명분을 홍보하고 조직원을 모집하며 정보를 얻거나 수익을 목적으로 사이버 커뮤니케이션 기술을 사용하는 것	

자료: 국가정보원, 사이버테러리즘(검색일: 2025.4.28.)

복합위협에서 사이버 공간은 위협을 전달하는 가장 주요한 수단 중 하나이다. 해양의 경우, 자율운항선박, 항만 자동화 등으로 최근 해양 사이버보안의 확보가 해양안전을 포함하여 국가 공급망 안보에 중요한 역할을 담당하고 있다. 특히, 해킹 등을 통해 국가전략 물자의 수출입 정보가 유출되거나, 수송선의 정보 또는 위치가 외부에 노출되면 국가 안보에 직접적인 영향을 미치거나 정보의 조작을 통해 사회 혼란이나 불안정을 야기할 수 있다. 반면, 사이버위협은 그 출처를 식별하기 어렵고, 공격이 발생한 후에도 그 주체를 특정하기 힘들어 대응이 매우 복잡하다.[68] 또한, 최근 첨단기술의 발달에 따른 인공지능 및 정보통신기술의 발전은 사이버위협을 더욱 정교하게 만들고 있다. 따라서 사이버위협의 효과적인 관리는 복합위협을 예방하거나 위협에 대한 대응력을 확보하는 주요한 정책적 수단이 된다.

68) 김소정, 앞의 책, p. 4.

〈표 2-5〉 해양 복합위협의 범위

구분	설명
해양 국제범죄	• 2개국 이상 또는 1개국에서 실행되었으나 그 과정의 중요한 부분이 다른 국가와 관련되거나 다른 국가에 효과를 미치는 중대범죄
해양테러	• 국가·지방자치단체 또는 외국 정부의 권한행사를 방해하거나 의무 없는 일을 하게 할 목적 또는 공중을 협박할 목적으로 하는 행위
해양 사이버위협	• 단순한 침해행위를 벗어나 정치·이념·종교적 동기를 지니고 정보시스템, 네트워크, 데이터를 공격하여 사회적 혼란을 야기하거나 특정 목표를 달성하려는 행위

자료: 저자 작성

2) 해양 복합위협의 유형

정리하면, 현재까지 우리나라는 해양 복합위협을 유럽 등 주요 선진국과 같이 국가의 정책적 차원에서 정의하거나 그 범위를 정하고 있지는 않다. 그러나 복합위협은 특정 목적의 실현을 위해 사이버 등 비물리적 수단과 폭발물 등 비물리적 수단을 함께 동원하여 위협을 가하는 행위를 의미하는 것이며, 해양 복합위협은 이러한 복합위협이 해양에서 발생하는 것으로 정의할 수 있다. 즉, 해양 복합위협은 해양 국제범죄, 해양테러, 해양 사이버위협이 복합적으로 나타나는 것으로 구체적인 유형으로는 자율운항선박 해킹 등을 통한 국가의 경제적 손실 유발, 드론 등을 활용한 해저케이블 등 해양 주요 인프라 공격으로 국가 사회 혼란 야기, 사이버 공격을 통한 테러범 동원 및 테러범 유입 유도, 사이버 공간을 활용한 해상 마약 거래 등이 있을 수 있다.

다만, 미국 해안경비대(USCG: United States Coast Guard), 영국, 유럽복합위협대응센터의 경우, 해양 복합위협 또는 해양에서의 위협의 구체적 유형을 정하기보다 최근 국제적으로 발생하고 있는 공격행위를 예시로 다음과 같이 해양위협을 제시하고 있다. 미국은 주요 해양 인프라 및 연안의 취약한 지역을 대상으로 해양에서 직접 공격할 수 있는 형태를 해양위

협으로 제시하고 있으며, 영국은 국가해양안보전략(NSMS: National Strategy for Maritime Security)을 통해 해양테러, 해상무역로 교란, 주요 연안 인프라 공격, 대량살상무기 등 불법 무기 밀수, 납치 및 인신매매 등 다섯 가지 유형으로 해양위협을 포괄적으로 제시하고 있으며, 유럽복합위협센터는 유럽 주변 해역에서 최근 발생하고 있는 주요 해양위협을 중점으로 해양위협의 형태를 제시하고 있다.[69]

〈표 2-6〉 국외 해양 복합위협의 유형

미국	영국	유럽복합위협센터
• 테러범 이송 • 무기 등 무허가 물질 밀수 • 여객의 폭발물 이송 • 선원 및 여객 납치 • 선박 등 해상 납치 • 납치 선박을 이용한 공격 • 선박 손괴 • 해양 인프라 손상 • 폭발물 테러 • 자동차 및 트럭 폭발물 공격 • 기뢰 공격 • 드론 공격 • 다이버 등을 통한 수중 공격 • 테러범 운송 • 납치 • 생화학 무기 등 대량살상무기 공격 • 사이버 공격 • 기타 국방부에서 정하는 공격 형태	• 영국의 해양이익에 영향을 미치는 테러 행위(선박에 대한 공격 행위 포함) • 전쟁, 범죄, 해적, 국제 질서 현상 변경으로 인한 주요 해상무역로 교란 • 영국 해양 인프라 또는 해운선사에 대한 공격(사이버 공격 포함) • 대량살상무기, 마약, 무기 등의 불법 해상운송 • 납치 및 인신매매	• 고속단정 공격 • 어뢰 등 수중 무기 공격 • 후티 등 무장단체 선박 공격 • 해양수송로 차단(사격 및 훈련 구역, 군사보호구역, 섬 주변해역 차단, 선박 검사구역 등을 통한) • 항해자유작전 등을 통한 타국 EEZ 항해 • 해저 가스관 공격 • 해저케이블 손상 • 해운선사 사이버 공격 • 항만, 해양플랜트 등 연안 주요시설 공격 • 해적 • 연안국 선박 억류(불법행위 주장을 근거로) • 불법조업(원양 및 EEZ 포함) • 불법 해양자원 개발(관할권 중첩 해역 포함) • 항만 등 연안 주요시설 사이버 공격

자료: Hybrid CoE(2025), pp. 9-10; Hybrid CoE(2023), pp. 12-63; HM Government(2022), p. 27; Brady Downs, LCDR(2008) 등을 참조하여 저자 작성

69) Hybrid CoE(2025), pp. 9-10; Hybrid CoE(2023), pp. 12-63; HM Government(2022), p. 27; Brady Downs, LCDR(2008) 등 참조

미국 등 해양 복합위협의 주요 국가들이 제시하고 있는 해양 복합위협의 형태를 고려하여, 해양 국제범죄, 해양테러, 해양 사이버위협의 대상 및 범위를 유형화하면 〈표 2-7〉과 같이 표시할 수 있다. 먼저, 해양 국제범죄는 해양경찰청, 출입국·외국인청, 관세청 등 법집행기관에서 관련 법령에 따라 현재 관리 및 대응하고 있는 범죄 유형으로서 밀입(출)국, 밀수(출)입, 납치, 해적 및 무장강도 불법조업, 해양오염 등과 같이 전통적인 해양위협으로 유형화할 수 있다. 이들 해양위협은 이미 제도적으로 대응체계가 수립되어 있어 고도화, 조직화, 전문화되고 있는 위협의 변화를 중심으로 제도 개선에 대한 논의가 필요하다.

다음으로 해양테러는 일반적인 「테러방지법」상 해양테러를 비롯하여, 최근 새로운 위협의 유형으로 등장하고 있는 해저시설 공격, 대량살상무기 위협, 드론 및 무인수상정 등을 활용한 무인체계 위협 등이 이에 포함될 수 있다. 4차 산업기술을 활용하여 물리적 위협까지 연결되는 행위로서 국가나 비국가 행위자가 특정 목표를 달성하기 위해 외교적, 군사적, 경제적, 기술적 수단 등 전통 및 비전통적 방법을 혼합하여 강제적·파괴적 활동을 행하는 것을 의미한다고 할 수 있다. 유럽 등 국제사회에서 해양 복합위협과 관련하여 국가 간 협력 등 가장 관심을 가지고 대응하고 있는 분야라 할 수 있다.

마지막으로 해양 사이버위협은 최근 해양 복합위협에서 가장 특징적인 위협 형태로 사이버위협 자체로도 많은 피해와 사회적 혼란을 야기하지만 사이버 공격을 매개로 해양테러 또는 해양 국제범죄가 발생할 경우, 위협은 사실상 국경을 초월하고, 행위자의 소재를 확인하기 어려우며, 피해자는 있지만 위협의 원인을 파악하기 어렵고, 자기과시 또는 행위 자체를 목적으로 위협을 실현할 경우 위협 발생 자체를 예측하기 어렵다.[70]

70) 송태은, 앞의 책, pp.6-7; 김소정, 앞의 책, pp. 2-3; 이 두 연구는 복합위협의 주요 수단이 되는 정보전 및 사이버 공격, 경제적 억압 등은 공격자의 식별을 어렵게 하고, 위험 한계가 국경을 넘을 수 있으며, 공격

〈표 2-7〉 해양 복합위협의 유형 및 행위

구분	유형	주요 행위
해양 국제범죄	• 밀입(출)국	• 무단이탈, 밀입국, 무사증, 밀항, 밀출국 등
	• 밀수(출)입	• 마약 밀수, 해양산업기술 유출, 불량식품 유통, 불법위폐 유통 등
	• 납치 및 인신매매	• 외국인 납치, 감금, 폭행 등
	• 해적 및 무장강도	• 금전적 이득을 위한 선박 나포 등
	• 불법조업	• 외국어선의 우리나라 관할 해역 불법조업 등
	• 해양오염 등 기타	• 선박 사고 등으로 인한 화물 및 연료유 유출, 난파선 침몰 등
해양테러	• 해양테러	• 연안 주요시설(발전소, 주요 항만 등) 위협, 연안 다중이용시설(여객선, 여객터미널 등) 공격 등
	• 해저시설 공격	• 해저케이블, 가스 수송관 등 공격
	• 대량살상무기 위협	• 대량살상무기 위협, 대형 환경오염 피해 등
	• 드론 등 무인체계 위협	• 드론, 무인 해상정 등을 활용한 연안 주요시설 위협 등
해양 사이버 위협	• 사이버침해 행위	• 랜섬 등 해킹 및 사이버 공격을 통한 선사 및 국가 기능 마비, 금전 요구, 허위정보 유포, 테러 행위자 모집, 사이버를 통한 사회적 혼란 야기 등

자료: 저자 작성

이에, 3절에서는 앞에서 유형화한 해양 복합위협의 사례를 분석하여 전통적 위협인 해양 국제범죄와 해양테러의 변화 양상과, 신흥 해양위협인 해양 사이버위협의 주요 쟁점을 도출하고 해양 복합위협에 효과적으로 대응하기 위한 시사점을 도출한다. 특히, 해양 국제범죄 등은 우리나라 관할 해역에서 발생한 주요 사례를 분석하여 국내 관련 제도를 개선하기 위한 취약점과 필요성을 도출하고, 해양테러와 해양 사이버위협의 경우 국내외 사례를 분석하여 이들에 효과적으로 대응하기 위한 정책적 시사점을 도출한다.

대상 또는 수단의 특정이 어려워, 테러 또는 위협의 행위자를 조사하고 수사하는 전통적 방식의 대응 전략은 복합위협에 적절하지 않을 수 있다고 주장

제3절 해양 복합위협 주요 사례 분석[71]

1. 해양 국제범죄 주요 사례 분석

1) 밀입(출)국 주요 사례 분석

(1) 중국인 일가족의 일본으로 밀출국 시도[72]

가. 사건 경과 및 개요

2025년 1월 19일 부산 기장군 공수항[73] 인근 항만수역 외 해상에서 중국인 30대 부부와 10대 자녀 두 명이 고무보트를 타고 일본으로 밀입국하려다 해양경찰청에 검거되었다.[74] 일가족은 2022년 7월 서해 표류 중 우리나라 공해에서 해군이 발견하여 한국으로 입국한 뒤 다시 일본으로 밀입국 시도 중 검거된 것으로 조사되었다.

나. 대응 및 후속 처리

우리 군이 해안 경계 중 밀출국 시도자를 발견하여 해양경찰청에 통보하였으며, 해양경찰청이 밀출국자 네 명을 체포하고 수사 후 출입국·외국인청(이하 출입국청)에 사건을 인계했다.

71) 제2장 제3절 해양 복합위협의 주요 사례 분석에서 1항(밀입(출)국 사례 분석)과 2항(마약 등 밀수(매) 및 불법 화물 해상운송 사례 분석)은 국내 사례를 중심으로 분석한다. 국내에서는 현재까지 해양 복합위협 발생 사례가 보고된 바 없어 본 장 해양 복합위협 사례 분석에서는 국외 사례를 중심으로 분석함

72) 채널A뉴스(2025.1.20.)(검색일: 2025.3.10.) 참조하여 저자 작성

73) 공수항은 부산 기장군 시랑리 공수마을에 위치한 어촌·어항법상 어촌정주어항으로 지정된 항구이다. 어촌정주어항은 어촌의 생활 근거지가 되는 소규모 어항을 의미함(한국어촌어항공단, 정주어항 현황(검색일: 2025.4.29.))

74) 채널A뉴스(2025.1.20.)(검색일: 2025.3.10.) 참조하여 저자 작성

다. 발생원인 및 시사점

「어촌·어항법」[75]상 어촌정주어항의 관리·감독 주체는 지방자치단체이지만 어항관리청은 어항의 유지·관리·운영에 관해 한국어촌어항공단, 지방공기업, 그 밖에 해양수산부령으로 정하는 자에 위탁할 수 있어 어항 지정권자와 어항 관리청의 이원화 문제점의 개선 필요성과 소규모 항포구를 통한 밀입(출)국 관리 한계점이 지적된 바 있다. 이에 따라 어촌정주어항과 같은 감시 취약 지역인 어촌정주어항에 기술 개발을 통한 저비용 고효율 감시센서 및 해상 드론을 도입하고, AI 알림 장비의 오경보 필터링 알고리즘 개선하여 탐지 정확도를 높일 필요가 있다.

(2) 인천 앞바다에 제트스키 밀입국 시도[76]

가. 사건 경과 및 개요

2018년 8월 16일 인천항[77] 국제여객터미널의 수상구역 내 갯벌에서 제트스키를 타고 중국에서 인천 앞바다로 밀입국을 시도한 중국 국적 남성이 검거되었다. 우리 육군 열상감시장비(TOD)가 제트스키를 타고 우리나라 해역으로 밀입국을 시도한 것을 탐지 후 경로를 추적하였으며, 인천대교 인근에서 제트스키가 멈춘 것을 파악하고 해양경찰청에 이상 선박 상황을 통보했다. 이에 인천해양경찰서는 현장에 공기부양정을 급파하여 밀입국 가능성을 두고 밀입국자의 신병을 확보했다.

75) 어촌·어항법 제16조(어항의 지정권자), 제35조(어항관리청 및 청항업무)에 어촌정주어항은 특별자치도지사, 시장·군수·구청장, 즉 기초 지방자치단체의 장이 지정하고 관리함을 명시하고 있다. 다만 어항관리청은 어항의 유지·관리·운영에 관해 한국어촌어항공단, 지방공기업, 그밖에 해양수산부령으로 정하는 자에 위탁 또는 대행할 수 있음

76) 한겨레(2023.8.21.)(검색일: 2025.3.10.) 참조하여 저자 작성

77) 인천항은 항만법상 국가관리무역항으로 지정되어 있으며, 인천항 국제여객터미널은 인천항의 항만시설로 분류되어 관리되고 있다. 인천항 국제여객터미널은 항만법 및 항만공사법을 근거로 하여 인천항만공사가 관리·운영하고 있음

나. 대응 및 후속 처리

우리 군이 해안 경계 중 밀입국 시도자를 발견하여 해경에 통보하였으며, 인천해양경찰서가 밀출국자 한 명을 검거 후 출입국청에 인계 조치했다.

다. 발생원인 및 시사점

이번 사건은 인천항 내 구역(수상)에서 인천항의 관리 주체인 인천항만공사와 인천항보안공사 외에 열상감시장비를 보유한 군, 해상 경비 장비와 인력을 보유한 해경, 출입국사범 고발권이 있는 출입국청이 협력하여 처리한 사례이다. 제도적으로 출입국청의 고발 없이는 형사절차가 진행되지 않는 현행 체계를 개선하여, 일정 요건 하에 해경이 고발 없이도 사건을 송치할 수 있도록 관련 법령 개정[78] 등 법적 보완을 검토할 필요가 있다.

(3) 서해 조업 어선의 밀입국 의심 선박 신고[79]

가. 사건 경과 및 개요

2025년 3월 8일 중국 산둥지역을 출항해 밀입국을 기도한 중국 국적자 두 명이 우리 영해에 들어오기 전에 해양경찰에 검거되었다. 인천해양경찰서는 인천 옹진군 소청도 인근에서 조업하고 있던 어선으로부터 영해 외측 해상에 수상한 선박이 있다는 사실을 수협중앙회 어선안전조업국을 통해 접수했다. 인천해양경찰서는 경비함정을 출동시켜 고무보트에 타고 있던 밀입국 시도자 두 명을 출입국관리법 위반 혐의로 긴급 체포해 인천출입국청에 인계했다.

78) 출입국청의 '초동 대응권' 강화 또는 해경에 대한 송치 권한 위임 검토(출입국관리법 제101조의 고발 요건 완화 혹은 공조 조항 신설)
79) 경기신문(2025.3.12.)(검색일: 2025.4.24.) 참조하여 저자 작성

나. 대응 및 후속 처리

어업인이 영해 외측 해상에서 조업 중 밀입국 시도자를 발견하여 어선안전조업국을 통해 해경에 사건을 접수하였다. 인천해양경찰서는 신고 해역 수색을 통해 밀입국 시도자 두 명을 검거 후 출입국청에 인계 조치했다.

다. 발생원인 및 시사점

해양경찰청은 해상 국경 범죄 예방을 위해 국내외 관계기관과 협조 체계 및 첩보·신고망 구축을 노력하고 있다.[80] 해양 보안을 강화하기 위해 군과 해양경찰청 외에도 어업인, 낚시객, 항만 근로자, 연안 지역 주민 등 민간 해역 이용자를 활용한 감시체계를 구축할 수 있다. 이들을 대상으로 밀입국 신고 홍보, 교육, 신고 포상금 지급 등을 통해 민간 협력 기반 확대가 필요하다.

(4) 인천항에 입항한 화물선의 선원이 항만 육상구역을 통한 밀입국 시도[81]

가. 사건 경과 및 개요

2023년 4월 2일 인천항에 정박 중인 화물선에서 베트남 국적 선원이 계선줄을 타고 항만 육상구역으로 무단 하선 후 밀입국을 시도했다. 인천항 보안공사는 항만 육상구역 감시 CCTV로 무단 하선을 확인한 후 현장 출동하여 야적장에 숨어 있던 해당 선원을 세 시간 만에 검거하여 인천출입국청에 인계했다.

나. 대응 및 후속 처리

항만보안공사, 해양경찰청 등 타 단속기관이 출입국사범을 검거하더라도

80) 해양경찰청은 지방청별 밀항·밀입국 대응반을 편성·운영하고 주말·공휴일·무월광 등의 취약 시간대 해상 경비를 강화하는 한편 밀항 · 밀입국 공익 신고자에 최대 1,000만 원 신고 포상금을 지급하고 있다(해양경찰청 보도자료(2024.5.3.)(검색일: 2025.9.9.)).

81) 경기일보(2023.4.25.)(검색일: 2025.3.10.) 참조하여 저자 작성

일반적으로 무단상륙 출입국사범은 「출입국관리법」[82]에 따라 출입국청에 인계하여 처리하고 있다.

다. 발생원인 및 시사점

항만보안공사의 감시를 통해 상황 발생 즉시 무단상륙 출입국사범을 검거하여 출입국청에 인계한 사건이다. 관련 법령 개정을 통해 관계기관 간 공조를 제도적으로 뒷받침할 수 있는 기반을 마련하고 항만보안 인력의 책임과 권한을 명확히 하여 물리적 대응이 가능한 구조로 재편할 필요가 있다.

(5) 인천항에 입항한 곡물운반선의 선원이 항만구역 철조망을 넘어 밀입국[83]

가. 사건 경과 및 개요

2021년 5월 2일 인천항에 정박 중인 곡물운반선에서 베트남 국적 선원이 항만 육상구역의 4m가 넘는 철조망을 넘어 밀입국했다. 그러나 밀입국자가 철조망을 넘어가는 모습이 주변 CCTV에 포착됐고, 알림 장치까지 작동됐지만 인천항보안공사 등 항만보안 관계자는 이를 파악하지 못했다. 다음날 선장은 해당 선원이 사라진 것을 인지하고 화물과 선원 수속을 대행하는 국내 해운대리점을 통해 관계 당국에 신고했고, 관계 당국이 밀입국 선원과 조력자를 검거했다.

나. 대응 및 후속 처리

선원의 무단상륙 및 밀입국 사건은 출입국청이 추적과 검거를 포함한 전체 처리 과정을 주도하여 처리한다. 출입국청은 고발을 통해 형사처벌 절

82) 출입국관리법 제14조(승무원의 상륙허가) 및 제101조(고발)에 따라 무단 입국(불법 상륙) 선원에 대한 주된 수사권과 처분 권한은 출입국·외국인청에 있다. 출입국사범으로 형사처벌을 위해서는 출입국·외국인청의 고발을 요하고 있어 해양경찰청은 초동 대응, 긴급 체포 등 물리적 검거는 가능하지만 출입국·외국인청의 고발 없이 사건을 자체적으로 송치할 수 없다.

83) YTN(2021.5.24.)(검색일: 2025.3.10.) 참조하여 저자 작성

차를 진행하며, 필요시 해양경찰청에 추가 지원을 요청할 수 있다.

다. 발생원인 및 시사점

항만보안을 위한 AI 감시 장비를 도입하고 있지만 움직임을 감지하는 장비는 감별 정확도가 낮다. 예를 들어 나뭇잎이 흔들려도 모니터링 시스템에 알림창이 나타나는데, 제한된 인력으로 이러한 모든 알림 경보를 확인하기에 한계가 있다. 이에 따라 정확도 및 신뢰도 높은 항만보안 감시기술 개발과 재발 방지 대책 마련이 필요하다.

(6) 인천항에 입항한 화물선의 선원이 항만 수상구역을 통한 밀입국 시도[84]

가. 사건 경과 및 개요

2019년 1월 2일 인천항에 정박 중인 화물선에서 방글라데시 국적 선원 두 명이 항만 내 수상구역으로 뛰어내려 무단 하선 후 밀입국을 시도했다. 인천항보안공사는 CCTV로 접안 선박 부근 해상에서 물체 이동을 감지했다. 인천항보안공사의 비상출동조가 현장 상황을 확인하고 해양경찰청 등 관계기관에 상황을 전파하였으며, 인천해양경찰서가 수상구역에서 해당 선원을 검거하여 인천출입국청에 인계했다.

나. 대응 및 후속 처리

선원이 묘박(해상) 중인 선박에서 수영하여 무단상륙을 시도하는 등 해상에서 상황이 발생하면 추적과 검거를 포함한 전체 처리 과정은 출입국청이 주도하여 담당한다. 그러나 필요시 해양경찰청은 해상 수색 등의 초동조치를 하고, 해상 인명 구조나 해양오염 등 해양경찰청 소관 업무가 연계된 경우 고발 이전까지의 조치를 수행한다.

84) 천지일보(2023.7.26.)(검색일: 2025.3.20.) 참조하여 저자 작성

다. 발생원인 및 시사점

해당 사건에서 항만보안공사는 CCTV로 이상 징후를 감지했지만, 해상에서 위반자를 직접 검거할 수 있는 수단이 부족하여 해상에서의 실질적 검거는 해양경찰청이 수행했다. 이에 대응하기 위해 제도 정비를 통해 해상 보안 주체 간 감시·경비 연계 체계를 강화하고, 해상 기반 위법 행위에 대해 초동 조치 권한과 범위의 명확화, 초동 조치 이후 출입국청으로의 이관 절차를 제도화하여 항만 내 수상구역 밀입국 시도에 대한 대응체계를 더욱 체계적으로 확립할 필요가 있다.

(7) 사례 분석 요약 및 시사점

가. 사례 분석 요약

밀입(출)국 사례에서 대응 대상이나 발생 장소와 관계없이 사건 발생의 인지 및 신고 주체는 군, 어업인, 항만보안공사, 화물선 선장 등 다양하게 나타났다. 그러나 사건 발생 장소가 수역이면 해당 구역의 관리 주체와 관계없이 해상에서 유일하게 물리적 조치가 가능한 해양경찰청이 수색, 검거, 현장 대응 등 초동 조치를 수행하고 있다. 초동 조치 이후에는 출입국사범의 형사처벌을 위한 고발 권한이 있는 출입국청에 사건을 이관하여 조사, 형사처벌, 강제퇴거 등 후속 처리를 한다.

사례 분석을 통해 밀입(출)국은 다양한 수단과 경로를 통해 발생하고 있는 상황과 대응 기관 및 주체별 한계를 확인했다. 밀입(출)국에 고무보트, 제트스키, 수영 등 소형·비정형 수단이 활용되고 있으며 비관리 취약지인 어촌정주어항, 무역항, 영해 외측 등 다양한 경로를 통해 발생하고 있음을 확인했다.

〈표 2-8〉 밀입(출)국 사례 분석 요약

구분	발생 장소	대응 기관 및 주체			발생 원인 및 협력 필요성					
		인지 및 신고	초동 조치 및 현장 대응	후속 처리	관할범위중복	정보공유미흡	인력/장비부족	법/제도미흡	기술한계	관리주체불명확
1	어촌정주어항 (항만구역 외 수역)	군 (해안경계)	해양경찰청 (해상 검거)	출입국·외국인청			○	○		○
2	국제무역항 (항만구역 내 수역)	군 (열상감시장비)	해양경찰청 (해상 검거)		○		○	○		
3	영해 외측 수역	어업인 (어선안전조업국 경유)	해양경찰청 (해상 검거)		○		○			
4	국제무역항 (항만구역 내 육지)	항만보안공사	항만보안공사 (육상 검거)		○			○		
5	국제무역항 (항만구역 내 육지)	선장 (해운대리점 경유)	해양경찰청 또는 출입국청 (육상 검거)				○		○	
6	국제무역항 (항만구역 내 수역, 안벽 옆)	항만보안공사	해양경찰청 (해상 검거)		○		○	○		

자료: 저자 작성

또한 여러 기관이 각자의 제한된 권한과 장비로 대응하고 있어, 해상 밀입국 대응에 있어 통합성과 효율성이 부족한 상황에 있음을 확인했다. 해양경찰청은 해상 범죄에 대한 유일한 경찰 세력임에도 비정형 수단의 탐지에 기존 장비는 한계가 있고, 해양경찰청은 수색 및 체포할 수 있지만 고발 없이는 출입국사범을 송치 불가하다. 출입국청은 출입국사범의 수사권 주체이지만 해상 단속 인력과 장비가 부족해 실제 현장 대응을 해양경찰청이나 군에 의존할 수밖에 없다. 항만보안공사는 무역항 항만구역 내 육상구

역에 대해 CCTV·경비 인력 등 시설 중심으로 대응하고 있으나 AI, CCTV 장비 경보 신뢰도가 낮아 실질적인 대응에 어려움이 있다.

현재 각 주체는 현장에서 관할 불명확성을 기관 간 협력을 통해 '인지 및 신고(항만보안공사/군/해양경찰청)' - '초동 조치 및 현장 대응(주로 해양경찰청)' - '사건 처리(출입국청)'[85]로 구분하여 처리하고 있다. 그러나 이러한 대응 방식으로 인해 출입국청, 해양경찰청, 군, 항만보안공사 간 사건 주도권이 불분명하고 역할이 분산되어 즉각적 대응에는 어려움이 있다. 또한 이러한 사건 처리 방식이 지속되어 정보·자산이 분산되어 있어 단일 기관 단독 대응에 한계가 있고 관계기관 협조 의존도가 높아지고 있는 구조이다. 그 외 군과 어업인 등이 중요한 탐지 임무를 수행하고 있으나 국가관리항 외 연안 지역, 지방자치단체 관리 항만은 감시 및 통제시설이 부족하여 어항은 보안이 취약한 점을 확인할 수 있다.

나. 시사점 요약

과거의 해상 밀입(출)국은 주로 밀항 알선책이 어선이나 화물선에 은닉시킨 뒤 공해상 등에서 선박 간 환승을 통해 이루어지는 방식이 일반적이었으나, 최근에는 국내·외 전문조직과 연계된 형태로 소형 · 고속보트를 이용하여 직접 밀입국을 시도하거나, 중고 수출 선박을 이용하여 밀항하는 등 그 수법이 날로 비정형화, 다양화되고 있다.[86] 밀입(출)국 대응의 핵심은 해상 경계선과 비공식 경로의 감시, 사각지대 해소에 있다. 이를 위해 무역항을 포함한 연안 지역의 보안을 강화하기 위한 법령 정비, 장비 확충, 감시기술 개발, 기관 협력 체계화, 민간 협력 기반 강화가 추진되어야 할 것으로 판단된다.

85) 해양경찰청이 초동 조치하여 출입국·외국인청에 인계한 사건의 경우 후속 처리 결과를 해양경찰청에 공유할 법상 근거는 없으나 업무 협조 차원에서 공유하고 있다(해양경찰청(2025.4.18.))
86) 경기신문(2024.5.2.)(검색일: 2025.4.24.)

2) 마약 등 밀수(매) 및 불법 화물 해상운송 주요 사례 분석

(1) 섬 지역 외국인 선원의 마약 유통·투약 사건[87]

가. 사건 경과 및 개요

2024년 11월 19일 서해지방해양경찰청은 전남 섬 지역 선착장에서 마약(일명 '던지기 수법') 유통책을 검거했다. 서해지방해양경찰청은 자체 첩보를 입수한 후 8개월간 수사를 통해 대마 3㎏을 압수하고 마약 판매책 네 명, 투약자 12명 등 태국 국적 외국인 노동자를 구속해 검찰로 송치했다.[88] 이어 국제 우편을 통해 마약 밀반입을 주도한 공급책과 총책을 검거하기 위해 수사를 지속하고 있다.

나. 대응 및 후속 처리

해양경찰청은 마약류 투약·판매 혐의가 있는 외국인 선원을 검거한 뒤, 관련 법률에 따라 수사하고 범죄 혐의가 확인되면 사건을 검찰로 송치한다.

다. 발생원인 및 시사점

이 사건은 외국인 노동자로 구성된 마약류 유통·투약 조직이 단속 사각지대인 섬 지역을 기반으로 운영되며, 국내 유통망과 국제 밀반입 루트까지 얽힌 국내외 마약범죄의 복합성을 보여주는 사례이다. 이에 대응하기 위해 국제 특송·우편이 마약 반입 수단으로 악용되는 새로운 유통 방식에 대응할 수 있도록 기술 기반 추적 시스템과 국제공조수사가 강화할 필요가 있다.

87) kbc뉴스(2024.11.18.)(검색일: 2025.3.10.) 참조하여 저자 작성
88) kbc뉴스(2024.11.18.)(검색일: 2025.3.10.)

(2) 외국인 선원 대상 마약류 유통 사건[89]

가. 사건 경과 및 개요

목포해양경찰서는 2024년 5월 말 외국인 선원을 상대로 마약류를 유통한다는 이주여성의 첩보를 입수했다. 목포해양경찰서는 첩보 입수 후 광주광역시 소재 유흥업소에서 근무하며 잠복, 탐문 수사를 이어가며 광주출입국사무소와 공조를 통해 마약류를 투약·판매하는 불법체류 외국인의 신원을 특정했다. 수사를 통해 목포해양경찰서는 2024년 7월 19일 엑스터시(MDMA) 및 케타민 등 마약 판매·투약자 세 명 및 중간 판매책 한 명, 2024년 9월 19일 상위 판매책 세 명, 2025년 1월 3일 마약 투약 장소 제공자 한 명 등, 총 여덟 명을 차례대로 검거했다.[90]

나. 대응 및 후속 처리

목포해양경찰서는 마약류 투약·판매 혐의가 있는 불법체류 외국인 선원을 검거한 뒤, 불법체류 여부를 확인하기 위해 출입국청에 해당 사실을 통보했다. 출입국청은 불법체류자인 외국인 선원의 형사처벌을 위한 고발장을 발부했다. 해양경찰청은 고발장이 접수되면 해당 외국인 선원을 형사입건하고, 관련 법률에 따라 수사하고 범죄 혐의가 확인되면 사건을 검찰로 송치한다. 출입국청은 필요시 출입국관리법에 따라 강제퇴거나 보호명령 등 별도의 행정조치를 취할 수 있다.

다. 발생원인 및 시사점

국내 불법체류 외국인의 증가와 출입국 시스템의 한계로 실시간 관리가 어려워지고 있다. 특히 불법체류 외국인은 취약한 신분 탓에 마약류 유통 같은 범죄에 노출되기 쉬우며, 이들을 매개로 외국인 판매책 등 국제 마약

89) 세계일보(2025.2.6.)(검색일: 2025.3.10.) 참조하여 저자 작성
90) 세계일보(2025.2.6.)(검색일: 2025.3.10.)

유통망과 연계 가능성도 있다. 그러나 단속과 수사 인력은 부족해 초기 범죄 정황을 포착하기 어렵고 내외국인이 혼재된 범죄에 특화된 정보 수집 및 감시체계도 미비한 상황이다.

이에 대응하기 위해 불법체류 외국인 밀집 지역을 대상으로 해양경찰청, 출입국청, 경찰 등 관계기관의 정기적인 합동 단속을 시행하고, 출입국청과 수사기관 간 협조를 통해 불법체류 외국인 범죄에 대한 형사·행정 절차를 신속하게 처리할 수 있도록 제도 개선이 요구된다.

(3) 국가관리무역항 입항 선박 내 마약 적발 사건[91]

가. 사건 경과 및 개요

2024년 4월 6일, 온산항[92]에 입항한 2만 5천 톤급 화물선의 따개비 제거 작업을 하던 잠수사가 씨체스트(일명 '기생충 수법')에서 마약 의심 물건을 발견하고 신고했다.[93] 신고를 접수한 대구본부세관을 현장 조사를 통해 코카인 블록(28.43㎏)과 블록에 부착된 위치추적장치(GPS)를 압수했다.

나. 대응 및 후속 처리

사건을 인계받은 대구지검은 선박 내·외부 수색, 선원 심문, 입출항 경로 분석, 미국 마약단속국(DEA)과 공조를 통해 수사를 진행했다.

다. 발생원인 및 시사점

이 사건은 국제 마약 밀매 조직이 선박의 구조와 입항 검사 절차의 사각지대를 악용해 마약 은닉 및 밀반입을 시도한 사례이다. 통상적인 입항 검사

91) 일요신문(2024.4.17.)(검색일: 2025.3.10.) 참조하여 저자 작성
92) 온산항은 울산광역시 울주군에 위치한 국가관리무역항으로 울산본항, 미포항, 울산신항과 함께 울산항의 항만시설에 포함된다.
93) 일요신문(2024.4.17.)(검색일: 2025.3.10.)

과정에서 씨체스트(sea chest)[94] 내부는 점검 대상이 아닌 점을 이용해 국제 운항 선박을 해상 밀수 수단으로 활용했다. 이에 대응하기 위해 입항 선박에 대한 수중 보안 점검을 정례화하고, 고위험 항로를 운항한 선박에 대해서는 표적 점검을 강화할 필요가 있다. 아울러 세관, 해양경찰, 검찰 등 관련 기관 간 정보 공유와 공조 체계를 제도화하여, 해양 밀수에 대한 대응력을 높일 필요가 있다.

(4) 지방관리무역항 입항 선박 내 마약 적발 사건[95]

가. 사건 경과 및 개요

2024년 4월 1일, 해양경찰청과 관세청은 미국 연방수사국(FBI)과 국토안보수사국(HSI)으로부터 강릉시 옥계항[96]에 입항하는 32,000톤급 벌크선[97]에 마약이 은닉되어 있다는 정보를 입수했다.[98] 2024년 4월 2일, 동해지방해양경찰청과 서울세관 마약 수사요원은 수색을 통해 선박 기관실 밀실에서 마약이 담긴 상자 수십 개(개당 약 20㎏)를 발견했다.[99] 동해지방해양경찰청과 관세청은 선원 20명에 대한 수사를 통해 국제 마약 밀매 조직과의 연계 여부도 조사했다.

나. 대응 및 후속 처리

해양경찰청은 증거 수집과 선원 심문을 통해 국제 마약 밀매 조직과 연

94) 씨체스트(sea chest)는 선박의 선체 하부(주로 바닥면)에 설치된 해수 유입구 구조물로, 선박 내 냉각수 공급, 평형수 주입, 소화설비 등에 사용되는 해수를 외부에서 끌어들이기 위한 공간이다.(현대중공업(주)(2014.1.14.), pp. 2-3 참조)

95) 세계일보(2025.4.2.)(검색일: 2025.4.25.) 참조하여 저자 작성

96) 옥계항은 강원자치도 강릉시 옥계면에 위치하며, 항만법상 지방관리무역항으로 지정되어 있다. 강릉시는 도내 기업 경쟁력 향상 및 강원권 물류 수요 대응을 위해 강릉시 옥계항 국제항로 활성화 지원 조례(2023.4.12.)를 제정하고 2023년 8월 옥계항에 컨테이너 국제 정기항로를 취항했다.

97) 해당 선박은 멕시코에서 출발해 에콰도르, 파나마, 중국 등을 거쳐 강릉시 옥계항에 입항한 벌크선이다.

98) 세계일보(2025.4.2.)(검색일: 2025.4.25.)

99) 세계일보(2025.4.2.)(검색일: 2025.4.25.)

관성을 추적하기 위해 인터폴 및 외교부와 연계한 국제공조수사를 추진 중이다. 관세청도 해당 선박의 기항지 세관과 정보 공유를 통해 공급망 추적, 국제 마약 운송 경로를 추적하고 있다.

다. 발생원인 및 시사점

이 사건은 국내 지방관리무역항으로 입항하는 국제 운항 대형 벌크선의 복잡한 구조와 항로 다양성의 특성을 마약 밀수 통로 악용한 사례이다. 이번 옥계항 사건은 지자체의 국제항로 활성화 정책과 달리 보안 인프라나 첩보 대응 시스템이 국가관리무역항 수준에 미치지 못해 발생하였다.

세관·출입국·검역(CIQ)을 전담하는 기관이 있는 국가관리항만과 달리 옥계항은 선박이나 화물을 확인하는 절차 없이 선원의 항만 외 구역 출입 시 몸수색을 하는 수준이다. 필요시 지방해양수산청이나 세관 등에서 출장을 나올 때도 있지만, 자체 시설이 없다 보니 제대로 된 검사 장비도 갖춰지지 않아 보안과 각종 범죄에 취약하다. 또한 지자체의 항만 통합관리 체계가 부재한 것도 사건 발생 원인으로 꼽힌다. 강원특별자치도는 옥계항의 관리청임에도 세관, 해양경찰청 등 관련 기관과 정보 공유가 없어 이번 사건에서 선박의 입출항 내역 외에 구체적인 정보를 파악하지 못하고 있었다.[100]

이에 대응하기 위해 국제항로를 운영하는 지방관리무역항에도 정밀 검색 장비와 전문 수사요원을 상시 배치하여 해상 마약 밀수 대응 역량을 높일 필요가 있다. 또한 지방관리무역항별 운영 규모 및 특성에 따라 필요시 「국제무역항」에 준하는 감시체계를 구축할 필요가 있다. 그 외 지자체, 관세청, 해양경찰청 등 관련 기관 간 정보 공유 체계를 마련할 필요가 있다.

100) 강원방송(2025.4.4.)(검색일: 2025.4.25.) 참조하여 저자 작성

(5) 환적 물류를 악용해 위조 상품을 밀반입·유통한 사건[101]

가. 사건 경과 및 개요

2023년 11월 7일, 인천해양경찰서는 2020년 11월부터 2021년 9월까지 266차례에 걸쳐 중국에서 생산한 위조 상품(정품 가격 기준 1조 원)을 밀수·유통한 조직을 적발했다.[102] 이들은 선박을 통해 들여온 화물을 항공기로 환적 중 컨테이너를 개방하여 화물을 분류한다는 점을 악용해 인천항으로 입항하는 컨테이너 화물선에 위조품을 환적화물로 위장해 들여오고 나서 인천국제공항 자유무역지역에서 위조 상품을 무단 반출하는 방식으로 밀수·유통했다.

나. 대응 및 후속 처리

인천해양경찰서는 관세법과 상표법 위반 혐의로 국내 밀수 총책, 사건에 가담한 인천국제공항 자유무역지역 보세창고 관계자 등 17명을 불구속 입건하고 검찰에 송치했다. 또한 국내에 밀수품을 공급한 중국 국적 두 명에 대해 인터폴에 적색수배를 요청했다.

다. 발생원인 및 시사점

이 사건은 자유무역지역 내 보세창고 환적화물의 허술한 관리, 관계기관 간 정보 공유 및 통합 감시체계 부재 등의 구조적 약점을 악용한 대규모 밀수 사건이다. 이에 대응하기 위해 관세청, 해양경찰, 공항공사, 검찰 등 관계기관 간의 상시 정보 공유 플랫폼 구축, 합동 조사팀 운영 정례화, 공항·항만 보세지역에 대한 공동 점검제도 도입을 검토할 필요가 있다.

101) 경인일보(2023.11.7.)(검색일: 2025.4.25.) 참조하여 저자 작성
102) 경인일보(2023.11.7.)(검색일: 2025.4.25.)

(6) 사례 분석 요약 및 시사점

가. 사례 분석 요약

국내 해양 공간에서 발생한 마약 밀수 및 불법 화물 운송 사례는 도서·연안 지역 외국인 선원의 마약 유통, 국제 무역항을 이용한 대규모 마약 은닉, 환적 물류를 활용한 위조 상품 밀반입 등 다양한 형태로 나타났다. 사례에서 사건 발생 시 주로 해양경찰청, 관세청이 초동 조치 및 현장 대응을 하고 검찰이 후속 처리를 하고 있음을 확인했다.

외국인 선원 중심의 마약 유통은 불법체류자 증가와 도서 지역 단속 사각지대를 배경으로 발생하였으며, '던지기 수법', 국제우편물 밀반입 등 교묘한 방식이 동원되었다. 선박을 통한 마약 밀수는 국가·지방무역항 모두에서 발생했으며 씨체스트(기생충 수법) 및 기관실 밀실 은닉 등 선박 구조의 사각지대를 이용한 방식이다. 또한 인천항과 인천공항을 연계한 환적 물류 체계를 악용한 위조 상품 밀수 사례에서 자유무역지역 보세창고 관리의 허점과 해상-항공 감시체계의 구조적 한계를 확인할 수 있었다.

〈표 2-9〉 마약 등 밀수(매) 및 불법 화물 해상운송 사례 분석 요약

사례	대응대상	발생 장소	대응 기관 및 주체			발생 원인 및 협력 필요성					
			인지 및 신고	초동 조치 및 현장 대응	후속 처리	관할범위중복	정보공유미흡	인력/장비부족	법/제도미흡	기술한계	관리주체불명확
1	선원	섬 지역 (전남)	해양경찰청 (자체 첩보)	해양경찰청 (수사, 검거)	검찰 (마약 처벌)		○			○	
2		연안 지역 (목포, 광주 일대)	해양경찰청 (이주 여성 첩보)	해양경찰청 (수사, 검거)	검찰 (마약 처벌), 출입국청 (불법체류 행정조치)		○	○			

사례	대응대상	발생 장소	대응 기관 및 주체			발생 원인 및 협력 필요성					
			인지 및 신고	초동 조치 및 현장 대응	후속 처리	관할범위중복	정보공유미흡	인력/장비부족	법/제도미흡	기술한계	관리주체불명확
3	선박	국가관리 무역항 (울산온산항)	잠수사 (따개비 제거)	세관 (현장 조사)	검찰 (마약 처벌)		○		○		
4		지방관리 무역항 (옥계항)	해양경찰청·관세청 (미국 첩보)	해양경찰청, 세관 (수색)	해양경찰청 (조사)		○	○	○		○
5	화물	보세창고 (공항)	해양경찰 청경	해양경찰청 (수사, 검거)	검찰 (처벌)		○	○			

자료: 저자 작성

나. 시사점 요약

해양 밀수 범죄에 대응하기 위해서는 선박의 은닉에 취약한 구조물과 도서·연안 지역처럼 단속이 어려운 구역에 대한 감시 및 단속 역량을 보강할 필요가 있다. 이를 위해 입항 선박에 대한 수중 보안 점검을 정례화하고, 위험 항로를 운항한 선박에 대해서는 선별검사 체계를 강화하는 등 선박 위험도 기반 점검 시스템의 도입이 요구된다. 아울러 외국인 선원들의 마약 유통 사례에 효과적으로 대응하기 위해서는 불법체류 외국인에 대한 실시간 관리 체계를 정비하는 한편, 해양경찰청, 출입국청, 경찰청 등 관계기관 간 정기적인 합동단속 체계를 구축하여 상시 모니터링 체계를 운영하고, 예방 중심의 단속 활동을 강화할 필요가 있다.

또한 지방무역항과 자유무역지역을 통한 해상 밀수 사례가 빈번히 발생함에 따라, 세관·출입국·검역(CIQ) 기능이 미비한 항만에도 정밀 검색 장비와 전문 수사 인력을 상시 배치하고, 보세창고의 관리 체계를 강화하기 위한 고성능 감시 장비와 자동화 시스템을 도입해야 한다. 나아가 해상과

항공 물류가 연계되는 과정에서 발생하는 복합형 밀수 범죄에 효과적으로 대응하기 위해서는 관세청, 해양경찰청, 출입국청, 공항공사 등 관계기관 간의 실시간 정보 공유 및 사건 공동 대응이 가능한 통합 플랫폼을 구축하는 것이 필요하다. 이와 함께 국제 마약조직과 연계된 범죄에 대응하기 위해 인터폴, 미국마약단속국(DEA) 등 국제 수사기관과의 협력체계를 확대하고, AI 기반 위험화물 탐지, 위성 위치추적, AIS 등 첨단 기술을 활용한 밀수 감시체계를 고도화할 필요가 있다.

2. 해양테러 및 해양 사이버위협 주요 사례 분석

1) 해양테러 주요 사례 분석

(1) 한-중 해저케이블 절단 사고[103]

가. 사건 경과 및 개요

2021년 10월 24일, 한국과 중국을 연결하는 국제 해저 통신망인 EAC(East Asia Crossing) 해저케이블이 중국해역에서 어업 활동 중이던 어선에 의해 물리적으로 절단되는 사고가 발생했다.[104] 이 케이블은 한중 간의 인터넷 트래픽 및 기업 간 전용 통신망 역할을 하고 있어 사고로 인해 일부 통신 서비스가 일시 중단되어 중국 내 한국 기업의 업무에 지장을 초래했다.

나. 대응 및 후속 처리

사고 직후 관련 통신사들과 국제 해저케이블 운영기관[105]은 손상 구간

103) YTN(2021.10.24.)(검색일: 2025.4.29.) 참조하여 저자 작성
104) YTN(2021.10.24.)(검색일: 2025.4.29.)
105) EAC(East Asia Crossing) 운영사는 글로벌 통신사 연합(국제 컨소시엄)이다.

을 확인하고 복구 절차에 돌입했다. 대한민국 해군과 중국해군은 복구 작업 주변 해역의 군사적 보안 상황을 감시했다. 우리나라 정부(과학기술정보통신부, 해양수산부, 외교부)는 국내 통신사와 협력해 네트워크 복구 상황 점검 및 국제망 우회 경로 확보 지원했으며, 중국 당국에 사고 원인 조사 협조 및 재발 방지 협력을 요청했다. 사고 이후 해양경찰청은 국내 해역에서 유사 사고 예방을 위해 케이블 보호구역 순찰을 강화했다.

다. 발생원인 및 시사점

이 사건은 어선이 해저케이블 보호구역[106] 내에서 불법 어망 또는 닻 사용으로 인해 케이블이 절단된 것이 직접적인 원인이다. 이는 해저 통신망이 어선의 물리적 간섭에 매우 취약하다는 점을 재확인시킨 사례로, 이에 따라 해양 내 해저케이블 보호구역에 대한 명확한 표시, 해양 이용자 대상 교육, 감시 기술의 확충이 필요함을 시사한다. 또한 장기적으로는 다중 경로 및 복원형 해저망[107] 설계와 같은 사이버안보 기반 인프라 강화도 병행되어야 함을 시사한다.

〈표 2-10〉 한-중 해저케이블 절단 사고의 기관별 대응 및 후속 처리

기관 및 주체		대응 및 후속 처리
대한민국 정부	과학기술정보통신부	• 국내 통신사와 협력해 네트워크 복구 상황 점검 및 국제망 우회 경로 확보 지원 • 전기통신사업법 제79조에 따른 해저케이블 경계구역 관리 실태 점검
	해양수산부	• 국내 해역 내 케이블 설치·표시 규정 준수 여부 확인 • 한국 해역에서의 추가 위험 요소 점검
	외교부	• 중국 당국과 협의해 사고 원인 조사 협조 요청 및 재발 방지 협력

106) 전기통신사업법 제79조(전기통신설비의 보호)에 해저케이블 보호를 위한 경계구역 지정, 표시 방법, 기간통신사업자에 경계구역의 위치를 자신의 인터넷 홈페이지 등에 공시 의무 등에 대해 규정하고 있다.

107) 복원형 해저망(Resilient Submarine Cable Network)은 자연재해, 물리적 손상, 사이버 공격 등으로 일부 구간이 손상되더라도 전체 통신망이 즉각적으로 다른 경로로 우회하여 기능을 유지할 수 있도록 설계된 해저 통신망 구조를 의미한다.

기관 및 주체		대응 및 후속 처리
중국 해양 당국 및 정부기관		• 사고 발생 해역 조사 및 사고 원인 파악 • 사고 어선의 불법 어망 사용 여부 조사 및 행정처분 • 한국 측과 외교 채널을 통한 정보 공유
민간	국내 기간통신 사업자	• 손상 구간 확인을 위한 국제 해저케이블 운영기관과 협력 • 우회 회선 확보(다른 국제 해저케이블망을 통해 트래픽 경로 재조정) • 네트워크 안정화 및 이용자 피해 최소화 조치
국제 해저케이블 운영기관		• 손상 구간 탐지(해저 광케이블 신호 분석) • 잠수함 케이블 전문 복구선 투입 및 엔지니어 파견
해양 경비 기관 및 군	대한민국 해양경찰청	• 국내 해역에서 유사 사고 예방을 위해 해저케이블 경계구역 순찰 강화
	중국 해경국 (China Coast Guard)	• 해당 어선 조사
	대한민국 해군, 중국 해군	• 직접적 복구 작업에는 참여하지 않았으나, 잠수함 케이블 주변 해역의 군사적 보안 상황 감시

자료: 저자 작성

(2) 영국 해저케이블 및 파이프라인 파괴 행위 대응을 위한 수중 드론 시험[108]

가. 사건 경과 및 개요

2025년 6월, 영국 국방과학기술연구소(Defence Science and Technology Laboratory)는 알포드 테크놀로지스(Alford Technologies) 등 민간업체와 협력해 개발한 고성능 원격조작잠수정(ROV: Remotely Operated Vehicle) 시험 운용을 시작했다.[109] 영국의 ROV 시험은 중국, 러시아 등[110]의 해저 위협 확대 속에서 해저 인프라 보호를 위한 원격 자

108) Naval Technology(2025.6.11.)(검색일: 2025.7.17.) 참조하여 저자 작성
109) Naval Technology(2025.6.11.)(검색일: 2025.7.17.)
110) 중국 상선이 발트해와 대만 해협 인근에서 의도적 케이블 절단에 연루됐다는 보고가 여러 차례 나왔으며, 2024년 3월 이후 발트해에서 최소 11개의 인터넷 케이블이 손상되었으며, 그중 일부는 러시아 선박에 의해 끌려간 것으로 추정되고 있다. (AP NEWS(2025.1.28.)(검색일: 2025.7.17.); Reuters(2024.12.4.)(검색일: 2025.7.17.) 등 참조)

동화 방어를 목적으로 해저케이블과 파이프라인에 대한 잠재적 위협(폭발물, 스파이 장비 등)을 감지하고 중화할 수 있도록 설계되었다.

나. 대응 및 후속 처리

영국은 포츠머스, 포틀랜드 항만, 남웨일스, 노르웨이 등 다양한 해역에서 ROV 시험 운용을 완료했으며, 시험 결과를 바탕으로 전술 매뉴얼, 운용 지침을 개발 중이다. 영국 국방과학기술연구소는 인력 투입 없이 원격으로 위험을 제거할 수 있는 플랫폼으로서, 해군과 민간 구조 부문 모두에 활용될 수 있다고 강조했다.

다. 발생원인 및 시사점

최근의 발트해와 대만 해협 일대 케이블 전단 사건에서 전통적 인력 중심의 폭발물 처리(EOD: Explosive Ordnance Disposal) 방식은 깊은 수심에서의 위협 대응에 한계를 확인했다. 이는 해저 인프라 위협이 증가에 따라 원격 자동화 방어 기술의 도입 시급성, 물리적 보안과 사이버 방어의 융합 필요성, 민간 인프라 보호를 위한 군·민 협력 모델 개발 필요성을 시사한다.

2) 무인체계(USV·ROV·드론) 기반 공격 사례

(1) 우크라이나의 러시아 공군기지 공격 '스파이더웹(Operation Spiderweb) 작전'[111]

가. 사건 경과 및 개요

2025년 6월, 우크라이나 정보기관(SBU)은 폭발물을 장착한 FPV 드론(UAV: Unmanned Aerial Vehicle)을 담은 컨테이너를 러시아 공군기지

111) AP NEWS(2025.6.3.)(검색일: 2025.7.17.) 참조하여 저자 작성

인근으로 반입한 뒤, 원격으로 컨테이너를 개폐하여 드론을 기지 내부에 침투시키는 방식으로 러시아 전략폭격기를 파괴 또는 손상했다. 우크라이나는 드론 117대를 사용해 러시아 공군기지 네 곳을 동시 공격하여 러시아 전략폭격기 41대(러시아 전력의 약 34~40%)에 피해를 줬다.[112]

나. 대응 및 후속 처리

러시아는 공격 직후 공군기지 주변의 경계를 강화하고, 군수기지 내부의 보안 점검을 했다. 또한 군수품 보관소와 항공기 주기장에 대한 이동식 방호벽 강화, 전자전(EW) 장비 배치, 드론 탐지 레이더 확충을 추진했다.

다. 발생원인 및 시사점

이 사건은 러시아 공군기지의 경계 시스템과 출입 통제 체계가 취약했기 때문에 발생했다. 특히 이번 작전은 단순한 원격 공격이 아니라, 군사적 목표를 식별하는 AI 기반 드론과 민간 물류(컨테이너)를 활용한 위장 전술이 결합한 형태였다. 이는 현대전의 양상이 변화하고 있음을 보여주며, 이러한 변화는 핵심 군사기지뿐만 아니라 항만, 해저케이블, 에너지 시설 등 중요 기반시설을 보호하기 위해 드론 탐지·차단 기술과 AI 기반 위협 식별 체계를 통합하는 등 물리적 보안과 사이버보안의 융합 관리가 필요함을 시사한다.

(2) 우크라이나의 무인수상정이 흑해 러시아 함선 공격[113]

가. 사건 경과 및 개요

2025년 5월 초, 우크라이나는 흑해 노보로시스크 인근에서 Magura V5 무인수상정(USV: Unmanned Surface Vehicle)으로 러시아 Su-30 전투

112) AP NEWS(2025.6.3.)(검색일: 2025.7.17.)
113) Business Insider(2025.5.4.)(검색일: 2025.7.17.) 참조하여 저자 작성

기를 격추했다. 해당 드론은 미사일을 탑재하고 자율 항법과 원격 조종으로 운용되었으며, 해상에서 공중 표적을 타격한 첫 사례로 기록되었다. 이는 기존의 자폭형 드론을 넘어, 해상 플랫폼이 공대공 미사일을 운용해 고가의 전투기를 무력화한 전술이다. 러시아는 Su-30 손실로 약 5천만 달러 이상의 피해를 보았다.

나. 대응 및 후속 처리

러시아는 공격 직후 러시아 군용기 조종사 일부를 민간 선박으로 구조하였으며, 노보로시스크 항만에 비상사태를 선포하고 방공체계 강화와 항만 보안 점검을 했다. 해당 사건은 우크라이나의 비대칭 전력 운용 능력을 극명하게 보여주는 사례로 해상 드론 전술의 혁신적 진화로 평가된다.

다. 발생원인 및 시사점

이 사건은 전통적 방공망이 해상에서 기습 발사되는 공대공 무기체계에서는 취약하다는 점이 드러났다. 해상 드론과 AI 기반 유도 기술의 결합은 물리적 보안과 사이버 방어를 통합한 새로운 대응체계 구축이 시급하다는 점을 시사했다. 또한 저비용·고효율 무기체계가 고가 자산을 무력화하는 비대칭 전력이 현대전의 핵심으로 부상했음을 보여주며, 국가 기반시설과 전략 자산 보호 전략의 재검토가 요구된다.

(3) 예멘 후티 무장세력 무인수상정의 미국 화물 선적 상선 공격[114)]

가. 사건 경과 및 개요

2024년 6월 12일, 홍해 남부 바브엘만데브 해협 부근에서 예멘 후티 반

114) U.S. Central Command(2025.6.12.)(검색일: 2025.7.17.); TWZ(2025.6.12.)(검색일: 2025.7.17.) 참조하여 저자 작성

군이 폭발물을 탑재한 자폭형 무인수상정(USV: Unmanned Surface Vehicle)을 이용해 상선 튜터호(MV Tutor)를 공격했다. 공격받은 선박은 라이베리아 선적이지만 미국 해운사와 관련 화물을 운송 중이었다. 공격 당시 튜터호는 항만 진입을 위해 속도를 낮춘 상태였고, 무인수상정(USV)은 고속으로 선체를 충돌해 폭발을 일으켰다. 이에 따라 선체가 심각하게 손상됐고, 선원 한 명이 실종됐다.

나. 대응 및 후속 처리

후티 반군의 공격 직후 미국 해군과 연합군은 홍해·아덴만에서 호위 작전을 강화했다. 미국 해군과 연합군은 구축함과 초계기를 투입해 인근 해역을 경계하고 추가 공격 가능성을 차단했으며, 항로 재편 및 안전항로 설정을 통해 민간 선박의 위험을 최소화했다. 미 국방부는 후티의 USV 제작·발사 거점을 정밀 타격했다. 미국은 IMO 결의[115]에 따라 선박 운항 지침을 개정[116]했다.

115) IMO 해상 안전 위원회(MSC)는 홍해와 아덴만에서 후티 반군의 상선 및 선원 공격(2023년 11월 MV Galaxy Leader호 공격 이후 2025년 7월까지 54건 공격 발생)에 대응하기 위해 제108차 회의(MSC 108, 2024.5.18.~24.)에서 홍해 지역 해상 안보에 관한 결의안(RESOLUTION MSC.564(108) SECURITY SITUATION IN THE RED SEA AND GULF OF ADEN RESULTING FROM HOUTHI ATTACKS ON COMMERCIAL SHIPS AND SEAFARERS)을 채택하고, 해상 사이버 위험 관리에 관한 개정 지침(MSC-FAL.1/Circ.3/Rev.3)을 승인했다.(IMO(검색일: 2025.8.25.))

116) MARAD는 미국적선의 남홍해·아덴만 통항 시 미 해군 중부사령부(NAVCENT)에 매시간 위치정보 제공, AIS 차단(AIS 지속 작동이 선박의 안전 또는 보안을 위협할 수 있다고 판단하거나 보안사고가 임박한 경우), NAVCENT의 항해 지침(NCAGS) 준수, 해당 해역 통항 시 미 해군과 항해 계획 조율을 요청(U.S.MARAD(검색일: 2025.8.25.))

〈표 2-11〉 예멘 후티 무장세력 무인수상정의 미국 화물 선적 상선 공격 사례의 기관별 대응 및 후속 처리

기관 및 주체		대응 및 후속 처리
미국 연방 정부	국방부 (DoD)	• 사건 브리핑을 통해 국제사회에 후티 공격 규탄 발표 • 해운업계에 위험 정보 제공 • 홍해 안전보장 강화, 무인체계 위협 대응 계획 마련
	교통부(DOT)	• 교통부 산하 해사청(MARAD: Maritime Administration)은 미국적 선의 남홍해·아덴만 통항 시 AIS 차단, 미 해군 중부사령부 (NAVCENT)의 항해 지침(NCAGS) 준수, 해당 해역 통항 시 미 해군과 항해 계획 조율을 요청
	미 해군 (U.S. Navy)	• 공격 직후 홍해 및 아덴만에서 호위 작전 강화(구축함, 초계기 투입) • 선박 항로 재편, 안전항로 설정 • USV 탐지·차단 장비를 추가 배치
	미 중앙사령부 (U.S. Central Command)	• 사건 상황을 실시간으로 파악하고 작전지휘 및 전술적 대응 • 후티 무장세력의 USV 발사 거점에 대해 정밀 공습 실시 • 연합군과 협력하여 위협 정보 공유 및 방호 대책 조정
연합군 및 국제 기구	연합 해군전력 (CMF: Combined Maritime Forces)	• 항로 보호 작전(Operation Prosperity Guardian) 강화 • 항만 접근로 및 정박지 순찰 강화 • 위협 징후 탐지 시 실시간 경보 발령
	국제해사기구 (IMO)	• 홍해 지역 해상 안보에 관한 결의안 채택, 사이버보안 지침 개정
예멘 정부 및 지역 당국		• 직접 대응능력 부족으로, 미·연합군에 정보 제공 • 지역 항만과 협력하여 의심 선박 및 무기 제작지 추적 지원
민간	해운사 및 선박 운영사	• 선박 운항 경로 변경 및 홍해 통항 연기 • 선박 자체 보안 조치(물리 장벽, 승무원 대피 훈련)

자료: 저자 작성

다. 발생원인 및 시사점

이 사건은 후티 반군이 저비용·원격 조종 USV을 활용해 항만 진입로와 정박 대기 구역 등 항만 인근에서 속도가 느린 선박을 표적으로 공격한 사건이다. USV은 소형·저피탐 특성으로 인해 기존 레이더망 체계로 탐지가

어렵고, 대응 시간도 제한되는 등의 항만 안보 취약성이 드러났다. 이에 따라 항만보안은 물리적 방어를 넘어 AI 기반 감시체계, 자동화 탐지·차단 장비, 국제 정보 공유 네트워크를 결합한 다층적 대응이 요구됨을 시사한다.

3) 항만·선박 사이버위협 주요 사례

(1) 시애틀 항만청 사이버 공격[117]

가. 사건 경과 및 개요

2024년 8월 24일, 시애틀 항만청은 Rhysida 랜섬웨어 조직에 의해 사이버 공격을 받았다. 이 공격으로 인해 시애틀-타코마 국제공항과 항만시설의 주요 IT 시스템이 중단되었다. 수하물 처리, 체크인 키오스크, 발권, Wi-Fi, 승객 디스플레이, 항만 웹사이트 등 다양한 서비스가 장애를 겪었다. 또한 약 90,000명의 이름, 생년월일, 사회보장번호, 운전면허증 번호, 일부 의료 정보 등 개인정보(워싱턴 거주자 71,000명)가 유출되었다.[118]

나. 대응 및 후속 처리

시애틀 항만청은 사고 발생 직후 주요 시스템을 오프라인으로 전환하고 네트워크를 분리했다. 사이버보안 전문가와 협력하여 사건의 원인과 피해 범위를 분석하고, 관계기관과 적극적으로 공조하였다. 대부분의 주요 시스템은 일주일 내 복구되었지만, 일부 웹사이트와 내부 포털은 복구 작업이 지연되었다. 항만청은 2025년 4월 3일, 사건에 대해 조사를 마치고 우편주소가 있는 피해자에게 개인정보 유출 개별 통지서를 발송하고 무료 신용 모니터링 서비스를 제공했다. 향후 유사 사건 방지를 위해 기존 시스템 교체 계획 수립하고 주정부 차원의 사이버보안 강화 조치를 위한 예산을 편

117) Port of Seattle(2024.9.13.)(검색일: 2025.4.29.) 참조하여 저자 작성
118) Port of Seattle(2024.9.13.)(검색일: 2025.4.29.)

성했다.

〈표 2-12〉 미국 시애틀 항만청 사이버 공격 사례의 기관별 대응 및 후속 처리

기관 및 주체		대응 및 후속 처리
미 연방 정부	사이버보안 및 기반시설 보안국(CISA)[119]	• 항만청과 협력하여 공격 유형 및 취약점 분석 • 국가 중요 기반시설에 대한 사이버위협 알림 발송 • 기술 지원팀 파견하여 사고 원인 조사·분석 및 복구 지원
	연방수사국 (FBI)	• 공격 조직(Rhysida 랜섬웨어 그룹)에 대한 범죄 수사 착수 • 국제범죄 네트워크 추적 및 랜섬웨어 암호화 키 탐색
	국토안보부 (DHS)	• 항만 운영 지속성 평가 • 항공·항만 물류 안전을 위한 보안 지침 강화
주 정부	워싱턴 주정부	• 피해 주민(약 71,000명) 개인정보 유출 대응 지원 • 무료 신용 모니터링 서비스 제공(항만청과 공동 제공) • 주정부 차원의 사이버보안 강화 조치 마련 및 예산 편성
항만 운영 기관	시애틀 항만청[120]	• 사고 초기 대응: 주요 IT 시스템 오프라인 전환, 네트워크 세분화 • 피해자 통보: 7개월 후 우편으로 개별 안내 및 보상책 제공 • 향후 조치: 보안 인프라 전면 점검, 기존 시스템 교체 계획 수립
민간	항만 운영 관련 IT·보안 업체	• 시스템 복구 및 보안 인프라 점검 지원 • 랜섬웨어 확산 차단 및 보안 취약점 패치 적용
군 및 해양 경비 기관	해안경비대 (USCG)	• 항만보안 관리 체계 및 해양운송보안법(MTSA: Maritime Transportation Security Act) 기준 검토 및 강화[121] • 직접적인 사이버 공격 복구에는 관여하지 않았으나, 항만 물리적 보안 강화를 위한 추가 순찰 및 점검 수행

자료: 저자 작성

119) 미 국토안보부 산하 사이버보안 및 기반시설 보안국(Cybersecurity and Infrastructure Security Agency)

120) 시애틀 항만청(Port of Seattle)은 워싱턴주법에 따라 설립된 특별 목적 공공기관으로 시애틀주 주민이 선출한 항만위원회(Port Commission)의 의결을 통해 항만 재정, 시설을 운영한다(Port of Seattle (검색일: 2025.8.25.)),

121) 2025년 7월 16일, 미 해안경비대(USCG)는 '해양 운송 시스템(MTS: Marine Transportation System)의 사이버보안에 관한 최종 규칙(이하 규칙)'을 발효했다. 이 규칙에 따라 미국의 모든 보고 대상 사이버사고는 지체 없이 국가대응센터(NRC)에 보고되어야 한다. 또한 2026년 1월 12일까지 해당 시설과 선박의 모든 직원은 사이버보안 교육을 이수하고 이후 매년 정기 교육을 이수해야 하며, 2027년 7월 16일까지 시설 및 선박 소유자·운영자는 사이버보안 책임자를 지정, 사이버보안 평가 수행, 사이버보안 계획 작성 및 승인 절차를 완료해야 한다(United States Coast Guard News

다. 발생원인 및 시사점

이번 사건은 공격자가 시애틀 항만청의 기존 시스템[122]이 랜섬웨어 공격에 취약한 점을 노려 데이터를 암호화하고 탈취한 사건이다. 이를 통해 항만 및 공항과 같은 국가 중요 인프라가 사이버 공격에 매우 취약하다는 사실을 확인할 수 있었다. 그러나 피해자 통보가 사건 발생 7개월 후 이루어진 점은 향후 신속한 대응체계 구축의 필요성을 시사한다.

(2) 호주 DP 월드 항만 사이버 공격[123]

가. 사건 경과 및 개요

2023년 11월 10일, DP 월드 오스트레일리아(DP World Australia)[124]는 자사 네트워크에 비인가 접근을 탐지하고, 즉시 인터넷 연결을 차단했다. 이에 따라 시드니, 멜버른, 브리즈번, 프리맨틀 등 주요 항만의 육상 운영이 중단되어 30,137개의 컨테이너가 항만에 적체했다. 11월 13일부터 항만 운영이 점진적으로 재개되어 11월 20일에 적체 컨테이너 처리를 완료했다.[125]

나. 대응 및 후속 처리

DP 월드 오스트레일리아는 사고 발생 직후 시스템을 오프라인으로 전환

(2025.1.17.)(검색일: 2025.8.18.)).

122) 기존 시스템(legacy system)은 오래되거나 구식 기술을 사용하여 구축된 컴퓨터 시스템, 소프트웨어 또는 하드웨어를 의미한다. 기술적으로는 구식이 된 시스템으로, 최신 보안 기준이나 기술 변화에 대응하기 어렵지만, 조직 운영에 여전히 필수적인 기능을 담당하고 있어 즉시 교체하거나 폐기하기 어려운 경우가 많다.

123) TXOne Networks(2024.1.22.)(검색일: 2025.4.29.) 참조하여 저자 작성

124) DP 월드 오스트레일리아(DP World Australia)는 두바이에 본사를 둔 글로벌 물류 기업인 DP 월드(DP World)의 자회사로 호주 해상 물류의 약 40%를 처리하고 시드니, 멜버른, 브리즈번, 프리맨틀 등 호주 주요 항만에서 컨테이너 터미널을 운영한다.(DP World(검색일: 2025.7.17.))

125) TXOne Networks(2024.1.22.)(검색일: 2025.4.29.)

하여 추가 피해를 방지하고, 사이버보안 전문가 및 호주 정부기관과 협력하여 사건을 조사했다. 조사 결과, 이번 사이버 공격은 호주 내 항만 서비스 서버에 대해서 이루어졌으며, 일부 직원의 개인정보가 유출되어 해당 사실을 피해 직원에게 통지하고 지원을 제공했다.

다. 발생원인 및 시사점

이 사건은 Citrix 시스템의 취약점으로 알려진 'Citrix Bleed'를 악용한 사건으로 취약점에 대한 패치가 제공되었음에도 DP 월드 오스트레일리아가 시스템에 적용하지 않아 공격에 노출된 것으로 조사됐다. 이 사건은 국가 중요 기반시설의 보안 취약성이 국가 물류에 큰 영향을 미칠 수 있음을 보여주며, 정기적인 보안 패치와 시스템 점검의 중요성을 강조한다. 또한, 사이버 공격에 대한 정부기관과의 협력 및 신속한 대응이 피해를 최소화하는 데 중요한 역할을 했음을 시사한다. 향후 유사한 사건을 방지하기 위해 공공 및 민간 부문의 협력을 통한 사이버보안 강화가 필요하다.

(3) 일본 나고야 항만청 랜섬웨어 공격[126]

가. 사건 경과 및 개요

2023년 7월 4일, 일본 최대 항만인 나고야 항의 중앙 시스템인 'Nagoya Port Unified Terminal System(NUTS)'이 랜섬웨어 공격을 받아 운영이 중단되었다. 시스템 장애로 인해 항만 내 다섯 개 컨테이너 터미널의 하역 작업 및 컨테이너 반출입이 전면 중단됐다. 이번 공격은 러시아 기반의 사이버 범죄 조직인 LockBit 3.0에 의해 수행된 것으로 추정되고 있다.

나. 대응 및 후속 처리

나고야 항만청은 사이버 공격 즉시 시스템을 차단하고 아이치현 경찰과

126) 파이낸셜뉴스(2023.7.5.)(검색일: 2025.4.29.) 참조하여 저자 작성

협력하여 사건을 조사했다. 7월 5일, 항만 당국은 랜섬웨어 감염 사실을 공식 발표하며 백업 데이터를 활용하여 시스템 복구 중이라 밝혔다. 7월 6일 오후부터 차례대로 터미널의 운영이 재개되어 저녁부터 정상 운영을 시작했다. 사건 발생으로 인해 이틀간 약 15,000개의 컨테이너를 운송하지 못해 항만 주변은 대기 중인 트레일러로 혼잡이 발생했다.[127]

〈표 2-13〉 일본 나고야 항만청 랜섬웨어 공격 사례의 기관별 대응 및 후속 처리

기관 및 주체		대응 및 후속 처리
일본 중앙정부 및 지방공공단체	국토교통성	• 일본 항만 운영 전반의 보안 지침 강화 지시 • 전국 항만에 대해 사이버보안 점검 긴급 지시 • 항만 물류 혼란 최소화를 위한 대체 물류 경로 지원
	경제산업성	• 자동차 수출 기업과 물류 대책 협의(특히 토요타 계열사 영향 분석) • 주요 무역 파트너국(미국, EU)과 물류 지연 정보 공유
	방위성	• 국가 중요 인프라 보호 정책 및 향후 사이버 방위 개념 강화에 대한 논의 • 일본 자위대의 직접 개입은 없었음(민간 인프라 사이버사고 성격)
	경찰청 및 아이치현 경찰	• LockBit 3.0 공격에 대한 수사 착수(기법 분석, 침투 경로 등) • LockBit 3.0 관련 국제범죄 데이터 공유 • 국제 수사 공조 요청(인터폴, 일본 내 사이버 범죄 대응팀 활용) 및 협력
항만 운영기관	나고야 항만청[128]	• 즉각 조치: 시스템 차단 및 네트워크 격리 • 복구 절차: 백업 데이터 기반으로 NUTS 재가동 • 운영 조정: 하역 중단 공지 및 물류 대기 트럭 관리 • 48시간 내 단계적 복구 완료, 저녁 이후 정상화 발표
민간	IT 서비스 및 보안업체	• 복구 과정 기술 지원 • 랜섬웨어 침투 경로 분석 및 패치 적용
	항만 운영 협력사 (물류기업)	• 대체 항로 확보 및 운송 지연 관리 • 고객사에 상황 공지 및 화물 추적 지원

자료: 저자 작성

127) 파이낸셜뉴스(2023.7.5.)(검색일: 2025.4.29.)

128) 나고야 항만청(Nagoya Port Authority)은 아이치현과 나고야시가 공동 출자하여 설립한 '특별지방자치단체'로 항만의 개발·운영·관리 등을 수행한다. 나고야 항만청 홈페이지(검색일: 2025.8.25.)

다. 발생원인 및 시사점

NUTS 시스템이 2023년 1월에 도입된 새로운 시스템임에도 불구하고, 보안 취약점이 존재했던 것으로 추정된다. 이 사례는 디지털화된 항만 운영 시스템의 보안 취약점을 드러낸 것으로 향후 유사한 공격을 방지하기 위한 보안 강화와 대응체계 구축의 필요성을 강조한다.

(4) 노르웨이 DNV 선박 관리(Ship Manager) 시스템 랜섬웨어 공격[129]

가. 사건 경과 및 개요

2023년 1월 7일, DNV는 자사의 Ship Manager 소프트웨어[130] 서버가 랜섬웨어 공격을 받은 것을 확인하고 서버를 즉시 차단했다. 이에 따라 약 70개 고객사와 1,000척의 선박이 온보드 오프라인 기능을 통해 기본적인 운영을 지속할 수 있었으나 온라인 서비스를 제공받지 못해 불편을 겪었다.

나. 대응 및 후속 처리

DNV는 공격 직후 Ship Manager 서버를 즉시 차단하고, 노르웨이 경찰 및 사이버보안 전문가들과 협력하여 사건을 조사했다. 조사 결과, 다른 시스템이나 데이터는 영향을 받지 않았으며, 사용자 계정, 이메일 등도 안전한 것으로 확인되었다. DNV는 고객사와 데이터 보호 당국에 서버 복구, 보안 체계 강화 조치 사항을 통보했다.

129) The Record(2023.1.17.)(검색일: 2025.4.30.) 참조하여 저자 작성

130) DNV社의 선박 관리(Ship Manager) 시스템은 전 세계 300여 개 해운사가 운영하는 7,000척 이상의 선박에서 사용되며, 선박의 기술적, 운영적, 규제 준수 측면을 관리하는 데 핵심적인 역할을 한다.(DNV(검색일: 2025.7.17.))

다. 발생원인 및 시사점

이 사건은 해양 산업에서 사용되는 소프트웨어의 보안 취약성을 드러낸 대표적인 사례이다. 특히, 선박 운영에 필수적인 소프트웨어가 공격을 받을 경우, 글로벌 공급망에 심각한 영향을 미칠 수 있어 해운사들은 소프트웨어의 보안 강화와 함께, 사이버 공격에 대비한 대응 계획 마련의 필요성을 시사한다.

(5) 해적의 CMS 해킹 및 고가 화물 약탈[131)]

가. 사건 경과 및 개요

2016년 해적들은 특정 화물선의 고가 화물만을 약탈하는 범행을 저질렀다. 해적은 사전에 해운사의 내부 화물 관리 시스템(CMS)을 해킹하여 고가 화물이 실린 선박과 컨테이너 정보를 확보하고, 선박에 침입해 해당 금품을 탈취했다. 해적은 해운사 CMS 웹의 보안 취약점을 통해 내부 정보에 접근했다.

나. 대응 및 후속 처리

해운사는 즉시 보안 전문 업체인 Verizon에 사건 조사를 의뢰하고, 서버의 악성 코드 및 웹 셸을 탐지해 제거했다. 또한 피해 서버 차단, 계정 비밀번호 재설정, 신규 웹 보안 스캔 및 패치 관리 체계를 도입했다.

다. 발생원인 및 시사점

이 사건은 해양 범죄가 단순한 무력 침입이 아닌, 정보전의 형태로 진화하고 있음을 보여주는 대표 사례이다. 사건의 주요 원인은 웹서버의 보안

131) 버라이즌 RISK(Research, Investigations, Solutions and Knowledge) 팀이 발표한 보고서를 바탕으로 작성된 Popular mechanics(2016.3.2.)(검색일: 2025.4.30.) 참조하여 저자 작성

기능 미비와 실행 권한 설정 오류였다. 이 사례는 선박 및 물류 운영 시스템의 디지털화로 인해 정보 보안과 접근 통제의 중요성이 더욱 커지고 있음을 시사한다. 이에 대응하기 위해 정기적인 보안 점검, 종사자 교육, 민간 기업의 보안에 대한 기술적 보완 조치가 필요하다.

4) 사례 분석 요약 및 시사점

가. 사례 분석 요약

해저 인프라 공격 사례에서의 경우, 해저케이블과 파이프라인은 광범위하고 심해에 위치해 있어 사고나 의도적인 절단이 발생해도 사전 예방하거나 실시간 감시가 어렵다. 사고 발생 시 데이터와 에너지 공급망이 동시에 마비될 수 있는 심각한 위험이 존재하며, 특히 복구에 장기간이 소요되어 경제적 손실과 국가 안보에 미치는 파급력은 매우 크다는 점을 확인했다.

항만 및 선박 사이버 공격 사례에서 운영시스템(OT)과 IT 망이 상호 연결되어 있어 보안 취약점이 발생하기 쉽고, 정기적인 보안 업데이트가 지연되는 경우가 많다. 이러한 환경에서 사이버 공격이 발생하면 하역 작업이 즉시 중단되어 공급망이 붕괴하고, 그 결과 경제적 피해가 급격히 확대된다. 더불어 민간 기업과 항만 당국 간에 명확한 위기 대응 프로토콜이 부재하여 초기 대응이 지연되고 피해 규모가 커지는 문제가 존재함을 확인했다.

무인체계 기반 공격(USV·ROV·드론) 사례에서 항만 진입로와 정박 구역에 있는 선박은 속도가 느려 공격에 매우 취약한 표적이 되었다. 특히 USV 공격은 기존 감시체계로 식별하기 어려워 방어가 쉽지 않았지만, 상대적으로 낮은 비용으로도 막대한 경제적 피해를 유발할 수 있어 해상 물류와 공급망 전반에 큰 파급효과를 미친다. 따라서 이러한 위험을 최소화하기 위해

서는 사전 예방 조치가 필수적이며, 이를 위해 AI 기반 탐지 기술, 다층 방어체계, 국제협력 강화 등 종합적 대응 전략이 요구됨을 확인했다.

나. 시사점 요약

우리나라는 해저 인프라, 항만·선박 사이버보안, 무인체계 기반 공격이라는 세 가지 주요 해양 복합위협에 직면할 위기에 있으며, 이에 대한 다차원적 대응 전략이 필요하다.

우리나라는 해저케이블과 파이프라인을 통한 데이터·에너지 네트워크 의존도가 높으므로, 해저 인프라 보호 강화를 위해 상시 감시체계 구축이 시급하다. AI 기반 해저 센서망과 위성 모니터링을 통합하고, ROV 및 자율수중체계(AUV)를 활용해 실시간 탐지와 긴급 복구 능력을 강화해야 한다. 또한, 해저 인프라 보호를 위한 국제협력 체계를 공고히 하여 NATO, ITU, IMO와의 협력을 통해 해저보안 합동훈련 및 정보 공유를 정례화할 필요가 있다. 더불어 국내 법·제도 정비를 통해 「전기통신사업법」상의 해저케이블 보호구역 관리와 해양 이용자에 대한 안전 교육, 그리고 민간통신사에 대한 보안 의무를 강화해야 한다.

또한 우리나라 항만은 스마트 항만화가 빠르게 진행되고 있어 사이버 공격 위험이 급증하고 있다. 따라서 항만 및 선박 사이버보안 강화를 위해 OT-IT 통합 보안 체계를 마련해 실시간 위협 탐지, 네트워크 세분화, 다중 인증을 의무화할 필요가 있다. 또한 IMO ISPS Code 개정을 반영한 국가 항만 사이버보안 지침을 강화하고, 항만공사·해운사·정부가 참여하는 공동 모의훈련을 실시해 대응력을 높일 필요가 있다.

항만구역에서 USV, 드론, ROV을 활용한 공격 가능성이 증가함에 따라 무인체계 기반 공격 대응을 위해 탐지·차단 능력을 강화할 필요가 있다. 아울러 AIS 데이터 인증 강화, 의심 선박 검문 등 출입 통제 절차 고도화,

한·미·일 및 동남아 국가와 정보 공유를 통해 해양안보 협력을 강화할 필요가 있다.

제4절 실효적 대응방안 필요성

본 장은 최근 해양위협의 국내외 경향과 동향을 분석하여 해양의 위협이 전통·비전통의 결합, 사이버와 연계, 동시다발적 발생으로 복합적인 양상으로 변하고 있음을 확인하였다. 그리고 본 장은 이러한 최근 위협 양상을 해양 복합위협으로 개념화하고, 위협의 대표적인 사례를 해양 국제범죄, 해양테러, 해양 사이버위협 등으로 유형화하여 조사 및 분석하였다.

해양 복합위협에 관한 논의 동향과 위협의 국내외 사례를 분석한 결과, 본 장에서는 해양 복합위협의 양상이 점점 다양화·비정형화되고 있는 반면, 현재 관련 국내 제도·장비·협력체계에는 위협에 효과적으로 대응하는데 한계가 있음을 확인하였다.

먼저, 해양 국제범죄 사례 조사 및 분석을 통해 하나의 연속적인 사건에서 다양한 정부 및 공공기관이 관할 구역 및 대상에 따라 분산된 기능을 수행하고 있는 것을 확인할 수 있었으며, 이렇게 개별 기관에 산재된 기능 및 역할은 단속의 사각지대 내지 책임 회피를 발생시킬 수 있음을 확인했다. 예를 들어 해양 국제범죄 중 가장 빈번히 발생하는 밀입(출)국 사건의 경우, 구체적인 상황에 대한 인지는 군, 어업인, 항만보안공사, 선장 등 다양한 주체에 의해 이루어지나 단속 등 초동 조치는 대다수 해양경찰에 의해서 이루어지고 있음을 확인했다. 사실 「국제선박항만보안법」에 따른 무역항 등 항만시설 지역의 경우, 항만공사, 지방해양수산청, 경비를 포함한

청원경찰 등이 초동 조치를 취하고, 권한 있는 기관에 사건을 인계해야 한다. 그러나 항만공사 등은 무역항 항계 내 수상구역에 대해 단속 및 대응 자원을 확보하고 있지 않아 해양경찰의 협조에 의존하고 있다. 또한 「국제선박항만보안법」이 적용되지 않는 일반 연안지역의 경우, 군 레이더 또는 해양경찰 함정을 통해 인지가 이루어지고 해상 단속 및 초동 조치는 해양경찰이 수행하고 사건의 처리는 법무부 출입국·외국인청을 통해 이루어진다. 이는 출입국 사범의 처리에 관한 권한이 출입국·외국인청에 주어져 있으나, 해상에서의 감시 및 대응 자원을 출입국·외국인청이 보유하고 있지 않아 해양경찰의 협조를 통해 대응이 이루어지고 있기 때문이다. 다만, 이러한 협력체계는 관할과 기능에 따라 개별 기관의 요청에 의해 이루어지는 것으로 신속한 대응에 제약이 있을 수 있다. 또한, 사건의 경중에 따라 책임의 회피 내지 단속의 사각지대가 발생할 우려 또한 존재한다.

다음으로 해양 국제범죄 사례 분석은 광범위한 해양에서 다양하게 발생하는 해양 복합위협을 제한된 국가 자산으로 상시적으로 감시하는 데 한계가 있음을 확인했다. 예를 들어 해상을 통한 밀수(출)입 사건은 해양경찰청과 관세청이 주로 대응하고 있으나, 관세청의 경우, 국제공항 및 항만, 통관센터, 물류거점 등에서 주된 단속을 실시하며, 기타 해상을 통한 일반 연안 지역의 밀수(출)입은 해양경찰청이 단속 및 검거를 실시한다. 특히, 관세청은 밀수 사범에 대한 처분에 관한 권한을 가지고 있는 반면, 기타 연안 및 해상에 대한 상시적인 감시 시스템을 갖추고 있지 않아, 사실상 도서 및 연안에서 발생하는 밀수 사건에 대해서는 해양경찰청의 단속 및 검거에 의존한다. 그리고 연안 및 해상에서 발생하는 밀수 사범과 관련하여서도 관세청 및 해양경찰청이 첩보를 통한 관련 범죄의 사전 인지가 부재할 시 관련 사건의 단속 및 처분은 어려운 상황이다. 더불어 밀수(출)입의 경우도 밀입(출)국과 유사하게, 관세청, 해양경찰청, 항공당국, 검역당국 등이 관할 및 대상에 따라 그 역할을 구분하여 대응하고 있어 단일의 사건에 유기적

이고 즉각적인 협력은 어려운 것으로 판단된다.

마지막으로, 최근 국제적으로 가장 활발하게 논의되고 있는 해양테러 및 해양 사이버위협과 관련하여 국외 사례를 조사한 결과, 신흥 해양 복합위협에 대응하기 위한 효과적인 대응체계 구축의 필요성이 확인되었다. 신흥 해양 복합위협은 국가 안보와 공급망에 중대한 영향을 미칠 수 있는 위협으로, 현재 국제사회에서 가장 중요한 논의 주제 중 하나로 부상하고 있다.[132] 예를 들어, 최근 발생한 해저케이블 절단 및 해킹 사고, 드론 등 해상 무인체계를 활용한 선박 및 연안 주요시설 공격, 항만 및 선박에 대한 해킹 등 사이버 침해 공격 사례는 국제 통신 체계를 일시적으로 마비시키거나, 주요 기반시설의 기능을 훼손하여 국가 해상 공급망에 심각한 영향을 미칠 수 있음을 보여주었다.

반면, 국내의 경우 이러한 신흥 해양 복합위협에 대응하기 위한 포괄적 국가 체계는 아직 미비한 것으로 보인다. 예를 들어, 2021년 한국과 중국 간에 발생한 해저케이블 절단 사고 당시 과학기술정보통신부, 해양수산부, 외교부, 국내 기간통신사업자, 해양경찰청 및 해군 등이 협력하여 사고 대응, 주변 해역 위험 조사, 외교 협상, 손상 복구, 사건 조사 등을 수행하였다. 그러나 이러한 협력은 주로 기관별 관할과 기능에 따라 사건 발생 이후의 사후 대응 중심으로 이루어졌으며, 위협의 예방-대비-대응-복구의 전 주기를 포괄적으로 관리하기 위한 체계적인 틀에 기반한 것은 아니었다.

현재까지도 국내에서는 신흥 해양 복합위협을 상시적으로 감시하고, 발생 가능성 또는 실제 발생 시 신속하게 상황을 전파하며 효과적으로 대응할 수 있는 관련 기관이 효과적으로 위협에 대응하는 조직적 체계가 확인되지 않고 있다. 특히, 신흥 해양 복합위협의 경우, 한 번의 발생으로 국가 안보와 국익에 막대한 영향을 미칠 수 있기에, 범부처 조직을 통해 다양한

132) United Nations General Assembly(2024), p. 21 등 참조

대응 기관의 기능을 조정하여 유기적인 협력을 통해 위협을 미연에 예방함과 동시에 즉각적인 대응도 가능하도록 국가적인 체계가 갖추어져야 한다.

〈표 2-14〉 실효적 대응방안 필요성 도출

검토 및 분석 내용		실효적 대응방안 필요성
해양 복합위협 국내외 논의 동향		• 위협의 다양화·비정형화
해양 복합위협 정의 및 범위		• 법적 정의의 부재
해양 복합위협 주요 사례	해양 국제범죄	• 요청에 의한 협력으로 기관 간 유기적인 협력 미흡 • 권한과 국가 자원의 불일치로 인한 대응 사각지대 발생 내지 책임 회피 가능성 존재
		• 관할 해역의 효과적 감시체계 미흡
	신흥 해양 복합위협(해양테러, 해양 사이버 침해)	• 포괄적 협력체계 미흡

자료: 저자 작성

이에, 3장에서는 해양 복합위협에 대응하기 위해 주요국들이 갖추고 있는 대응체계와 제도를 검토하고, 향후 국내적으로 해양 복합위협에 효과적으로 대응하기 위해 갖추어야 하는 요소들을 살펴보고자 한다.

03
해양 복합위협 대응체계 국외 사례 분석

본 장에서는 미국, 일본, 영국 등 주요국의 해양 복합위협 대응체계를 검토한다. 주요국은 해양 복합위협에 관한 포괄적인 제도를 수립했다. 미국은 국토안보부와 법무부, 국방부를 중심으로 기존의 해양 국제범죄뿐 아니라 새로운 복합위협의 유형에 따라 유기적인 협력체계를 구축하고 있다. 영국은 내각 산하에 해양안보 대응체계를 구축하고 있으며 부처·기관의 기능별 역할을 규정하여 대응하는 제도를 구축하고 있다. 뿐만 아니라 미국과 영국은 북대서양조약기구(NATO, North Atlantic Treaty Organization)와 EU를 중심으로 2017년 유럽복합위협대응센터를 설립을 주도하기도 했다.[133] 일본은 해역에서 발생하는 여러 유형의 위협에 대응하는 일원화된 체계를 구축하고 있다. 미국은 유관기관 간 고도의 유기적 통합을, 영국은 다기관 분산형의 제도적 결합을, 일본은 권한 명시를 통한 실행 권력 중심의 일원화를 눈여겨볼 만하다. 본 장에서는 이들 주요국이 해양 복합위협에 대응하는 법제, 기관별 역할, 거버넌스를 분석하여 향후 우리나라 해양 복합위협 대응체계 개발과 제도개선 방안에 대한 시사점을 도출하고자 한다.

133) Hybrid CoE, Establishment(검색일: 2025.4.28.) 2016년 EU/NATO 공동 선언을 통해 유럽복합위협대응센터 설립에 합의하고, 2017년 4월 11일 영국, 미국, 핀란드, 스웨덴, 라트비아, 리투아니아, 폴란드, 프랑스, 독일 등 9개국의 참여로 센터를 설립. 현재 36개국이 참여하고 있으며, 해양 복합위협을 포함하여 분야별 복합위협에 관한 제도, 정의, 범위, 관련 사례 등을 다양하게 제공

제1절 미국의 해양 복합위협 대상과 대응체계

1. 관리 대상 및 범위

미국은 다양한 형태의 테러 위협, 이주와 초국경 조직 범죄, 사이버위협, 지정학적 전략 경쟁 등에서 야기되는 국토 안보 위협을 '공공안전과 안보', '국경과 이주 안보', '주요 기반시설 안보', '경제 안보'로 구분한다.[134]

〈표 3-1〉 미국 국토안보부의 안보와 위협 분류

안보 유형	위협 내용
공공안전과 안보	테러, 마약, 영향력 작전과 초국가적 탄압
국경과 이주 안보	이민, 초국경 범죄 조직
주요 기반시설 안보	사이버 공격, 물리적 공격, 첩보 수집
경제 안보	경제적 조작과 강압, 경제적 첩보 활동

자료: Department of Homeland Security(2024) 내용 참고로 저자 작성

'공공안전과 안보'는 테러와 마약뿐 아니라 러시아·이란·중국의 영향력 작전과 초국가적 탄압을 포함한다. '국경과 이주 안보'는 이민과 초국경 범죄 조직에 관한 것이다. '주요 기반시설 안보'는 사이버 공격, 물리적 공격, 첩보 수집을 구분하고 있다. '경제 안보'는 시장·통화 등의 경제적 조작과 강압, 산업 스파이 등의 경제적 첩보 활동을 말한다. 이상 네 가지 안보 위협과 관련하여 해양에서 발생할 수 있는 대표적인 유형을 정리하면 〈표 3-2〉와 같다.

134) Department of Homeland Security(2024)

〈표 3-2〉 해양에서 발생하는 위협의 대표 유형

위협 유형	설명
해양테러	대량살상무기 밀반입, 폭발물·자살선박
항만·선박 공격	각종 선박 및 항만 기반시설 공격
불법활동	밀수, 인신매매·불법 이민, 해적·납치·강제 점거
복합위협	테러리스트 침투, 내부자 위협, 사이버위협
환경위협	해양오염, 불법어업

자료: Downs(2008)을 참조하여 저자 작성

미국 국토안보부는 2025년에도 남아메리카와 중앙아메리카, 카리브 해상로를 통해 미국 본토로 이동하는 해상 마약 밀수가 지속될 것으로 예상한다.[135] 주요 경로는 에콰도르-콜롬비아-카리브해와 멕시코만-본토이며 멕시코, 에콰도르, 콜롬비아 카르텔이 협력하는 것으로 보인다. 해상 경로는 지상 국경보다 단속이 어렵고 대상 운송이 가능하기 때문에 카르텔이 선호하는 밀수 방식이다.

항만 인프라 위협은 중국의 항만 투자와 운영 통제에 따른 전략적 영향력 확대를 우려하고 있다.[136] 중국이 페루 찬카이 항구 등 중남미 지역 항만 인프라에 대규모 투자를 진행하고 있기 때문이다. 중국이 해운 및 공급망에 대한 통제를 강화하여 미국과 동맹국의 해상 물류 안전성에 간접적 위협을 가하고 있다고 보고 있다.

해상교통 인프라 위협에 대한 직접적인 수치는 제시되지 않았지만 ISIS 및 알카에다가 교통 인프라를 주요 공격 목표로 삼은 점, 2023년 10월 하마스 테러 이후 다양한 극단주의 세력이 교통 인프라를 공격 대상으로 삼고 있다는 점이 주목된다.[137]

135) Ibid., p. 18.
136) Ibid., p. 30.
137) Ibid., p. 24.

2. 관리제도 및 대응체계

1) 주요 법률 및 제도

미국의 해양 복합위협 대응 법·제도는 2002년 제정된 해양운송보안법을 통해 물리적 보안에 역점을 두었다. 이후 컨테이너 보안, 세관-무역 보안, 항만보안, 화물 안전 등으로 법제가 확대되었다. 2024~2025년에는 사이버위협에 대응하기 위한 법제를 행정명령과 규정을 통해 보완했다.

(1) 해양운송보안법(MTSA)

해양운송보안법(MTSA: Maritime Transportation Security Act)은 미국 항만과 해상운송의 보안을 강화하기 위한 기본법이다. 2002년 9.11 테러 이후 항만과 선박이 추가 공격을 받을 우려로 인해 제정되었다.[138] 국제선박 및 항만시설 보안규칙(ISPS Code)과 함께 발전했지만 미국은 자체적으로 국내 항만과 선박에 더 폭넓게 적용하고 있다.[139] 이 법에 따라 항만시설과 선박 보안 계획을 수립하고 집행한다. 각 항만시설은 보안평가를 기반으로 보안 계획을 수립하고, 이를 해안경비대(USCG)에 제출하여 승인을 받아야 한다. 또 미국을 출입하는 선박은 보안 계획을 수립하고, 선박 보안 책임자를 지정해야 한다.[140]

(2) 컨테이너 보안 이니셔티브(CSI)

2002년에 미국 세관국경보호청(CBP)이 시작한 컨테이너 보안 이니셔티브(CSI: Container Security Initiative)는 미국으로 들어오는 해상 컨테이너 화물의 보안을 강화하기 위한 국제협력 프로그램이다. 이는 미국으로

138) McNicholas(2016), p. 120.
139) Ibid., pp.120-121.
140) United States Coast Guard, ISPS/MTSA(검색일: 2025.8.14.)

들어오는 화물의 보안을 강화하고, 위험 요소를 사전에 차단하는 것을 주요 목적으로 한다. 위험 분석 및 선별, 사전 검사, 국제협력을 주요 내용으로 한다. 우선, 미국으로 향하는 컨테이너 중 위험도가 높은 화물을 출발지 항구에서 선별한다. 다음으로, 선별된 컨테이너는 미국 도착 전에 출발지에서 사전 검사를 실시한다. 마지막으로, 해외 주요 항만에 CBP 요원을 파견하여 현지 세관 당국과 협력한다.[141]

(3) 세관-무역 파트너십(C-TPAT)

세관-무역 파트너십(C-TPAT: Customs-Trade Partnership Against Terrorism)은 미국 CBP와 민간 기업 간의 자발적인 파트너십이다. 국제 공급망의 보안을 강화하기 위해 2001년에 도입되었다. 정부와 민간 기업이 협력하여 공급망의 보안을 강화하는 것이 주요 목적이다. 기업은 보안 기준을 준수하고 CBP가 이에 대한 지원 및 혜택을 제공한다. 참여 기업은 CBP가 제시한 보안 기준을 준수하고, 자체 보안 관리 체계를 구축한다. CBP는 참여 기업에 대해 통관 절차 간소화 등의 혜택을 제공한다.[142]

(4) 항만보안법(SAFE Port Act of 2006)

항만보안법(SAFE Port Act of 2006: Security and Accountability For Every Port Act)은 MTSA 시행 과정의 제도적·운영상 한계를 보완하기 위해 2006년에 제정된 추가 보완법이다. MTSA가 개별 선박과 항만보안에 초점을 두었다면, 항만보안법은 CSI와 C-TPAT를 강화하고 외국 항만 평가·인증제를 포함하여 국제 공급망과 연계한다.[143]

141) U.S. Customs and Border Protection, CSI: Container Security Initiative(검색일: 2025. 8.14.)
142) U.S. Customs and Border Protection, Customs Trade Partnership Against Terrorism (CTPAT)(검색일: 2025.8.14.)
143) Ibid., pp. 133-134.

(5) 화물 안전 이니셔티브(SFI)

화물 안전 이니셔티브(SFI: Secure Freight Initiative)[144]는 SAFE Port Act of 2006의 후속 조치로 도입한 국제 해상화물 보안 강화 프로그램이다. 미국행 컨테이너 화물에 대해 출항지에서 사전 스캔한다.

(6) USA Freedom Act of 2015 – Title VIII

해상항법의 안전과 해양테러 방지 조항을 포함하고 있다.[145] 선박이나 해양 고정 구조물에 대한 핵무기·방사능·화학·생물무기 사용, 무기 수송, 사람에 대한 위해 행위 등에 대한 엄격한 형사 처벌을 명시한다.

(7) Executive Order 14116

2024년 2월에 발표된 행정명령(Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States)으로 선박·항만·해안 시설에 대한 사보타주, 지하 활동, 위협적인 사이버 사건을 보고하도록 규정하고 있다.[146]

(8) Coast Guard Final Rule: Cybersecurity in the Marine Transportation System

미국의 해양 지배력 회복을 위해 MTSA를 확대하는 조치로 2025년 1월에 발표, 7월 16일부터 발효되었다. 미국 국적 선박, 외변대륙붕 시설, MTSA의 적용을 받는 시설에 최소한의 사이버보안 요건(사이버보안 계획 수립, 사이버보안 담당자 지정, 사이버사고 보고 등)을 도입하게 했다.[147]

144) Ibid., p. 132.
145) Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015.
146) Federal Maritime Commission(2024.2.25.).
147) United States Coast Guard News(2025.7.16.)(검색일: 2025.8.13.)

〈표 3-3〉 해양 복합위협 관련 미국 연방 법률

구분	법령	설명
밀수(출)입	Tariff Act of 1930 (19 U.S.C.)	• 불법 수입품, 밀수품 압수·처벌
	Smuggling Statute (18 U.S.C. § 545)	• 허위신고·밀수입 처벌·규제
	Maritime Drug Law Enforcement Act(MDLEA) (46 U.S.C. § 70501-70508)	• 미국 영해뿐 아니라 국제 수역에서 마약 밀매 단속
	Drug Trafficking Vessel Interdiction Act of 2008(DTVIA) (46 U.S.C. § 70508)	• 무국적 자항식 반잠수정(SPSS: Self-Propelled Semi-Submersible) 및 잠수정 이용 마약 밀매 단속
밀입(출)국	Immigration and Nationality Act 8 (U.S.C. § 1324-1327)	• 외국인 밀입국 조장·은닉·운송 • 무단 국경통과, 밀항 등 처벌 • 강제추방 후 재입국 시 가중 처벌
	Criminal Sanctions for Failure to Heave to, Obstruction of Boarding, or Providing False Information (18 U.S.C. § 2237)	• 해상 단속 중 정지 명령 불이행, 검문 방해, 허위 진술에 대해 처벌
테러	1983 Act to Combat International Terrorism	• 미국 국민에 대한 국내외 테러 범죄 포괄, 국제테러 대응
	Antiterrorism and Effective Death Penalty Act of 1996	• 미국 내 테러 행위를 연방범죄로 규정, 연방정부의 테러 수사관 강화
	USA PATRIOT Act 2001	• 9.11테러 이후 법집행기관의 수사 권한 대폭 확대
	Homeland Security Act of 2002	• 반테러 기능의 통합·효율화를 위해 국토안보부 창설
	18 U.S.C. Chapter 113B	• 항공기 폭파, 테러 조직 지원, WMD 사용, 컴퓨터 해킹, 핵·방사능 관련 등 테러 행위 규율
사이버 위협	National Cybersecurity Protection Act 2014	• 연방·주·지방·민간 부문 전반의 사이버위협 대응 협력체계 마련
	Cybersecurity Information Sharing Act 2015	• 연방 차원 기본법 • 기업-정부 간 정보 공유 보호
	Cybersecurity and Infrastructure Security Agency Act 2018	• 국가 중요 기반시설 보호와 사이버위협 대응 주관

자료: 코넬대 로스쿨 법령정보센터(검색일: 2025.8.13.); 박용기(2006), pp. 7-9.

2) 기관별 역할

(1) 국토안보부(DHS)

미국에서 복합위협에 대한 대응체계가 체계적으로 조직된 것은 2002년 9.11테러 이후이다. 국토안보부(DHS: Department of Homeland Security)는 미국의 내부 보안 역량이 분산된 문제를 해결하고자 22개 연방 기관을 통합한 부처이다. 국토안보부 산하에 해안경비대(USCG), 세관국경보호청, 이민세관단속국을 비롯해 연방비상관리청까지 이관되었다.[148] 해상 단속-수사-이민 통제-재난 대응을 통합 수행할 수 있다. 국토안보부의 대테러 업무는 국가정보국(Office of the Director of National Intelligence) 산하 국가대테러센터(National Counterterrorism Center)에서 수집된 정보를 기반으로 한다.[149]

가. 해안경비대(USCG)

해안경비대(USCG)는 항만과 해상에서의 불법 활동을 방지하는 미국의 해양보안 주무기관이다. MTSA에 따라 항만과 선박의 보안 계획을 검토하고 승인한다. 해상 밀입국, 밀수, 테러 등의 위협에 대응하기 위해 순찰과 단속을 수행한다. 또한 항만과 선박에 대한 정기적인 보안 검사를 실시한다. 대형함정에는 해상법집행팀이 승선하여 현장에서 활동한다.[150]

USCG는 9·11테러 이후 국가 안보 관련 정보 수집 기능과 책임을 부여받아 인간정보·기술정보 등 정보 수집 분야별 임무를 전문화하고 있다.[151] 동·서해안에 해양첩보융합센터(Maritime Intelligence Fusion Centers)를 설치했으며 주요 항구에 현장정보지원팀을 파견한다.[152] 암호정보단

148) Department of Homeland Security(검색일: 2026.1.19.)
149) 함혜현(2022), p. 181.
150) 해양경찰청(2025.3.25.)
151) 함혜현, 앞의 논문, p. 187.
152) 위의 책, p. 182.

(Cryptologic Group)과 해안감시부(Coast Watch)를 설치하고 방첩 업무를 강화했다.[153] 기존의 치안 및 수색구조 서비스에서 대테러 중심 조직으로 전환하면서 2008년에는 명실상부한 정보기관으로 거듭났다.[154]

해안경비대(USCG)는 수사, 정보, 특수부대, 항만국 통제(PSC) 기능을 모두 가지고 있어 군인과 일반직이 있다.[155] 수사국은 감찰업무를 주로 하며 피의자 검거 시 마약, 안보 담당 연방정부기관에 이송하여 처리한다.[156] 특별사법경찰권을 보유하고 있어 해상에서 도주한 피의자를 해안까지 추격하여 육지에서 법집행을 할 수 있다.[157] 특수부대는 대테러, 해적 대응, 범죄 진압, 핵·생화학무기 해체 등의 임무까지 수행한다.[158]

나. 세관국경보호청(CBP)

미국 세관국경보호청(CBP: Customs and Border Protection)은 국경보안과 통관 절차를 담당하는 기관이다. 미국의 국경과 항만을 보호하고 불법 활동을 차단하는 역할을 한다. 화물 검사 및 통관, CSI 및 C-TPAT 운영, 밀수 및 밀입국 단속을 수행한다. 미국으로 들어오는 화물에 대한 검사와 통관 절차를 수행하여 불법 물품 반입을 방지한다. CSI와 C-TPAT을 운영하여 국제 공급망의 보안을 강화한다.[159]

153) 위의 책, p.182.
154) 위의 책, p. 187.
155) 해안경비대법(Title 14 of the United States Code – Coast Guard: U.S.C Title 14)에 따르면 항만보안과 해상 밀수 외에도 해양사고 예방, 유해 물질 운반·관리, 해양생물자원 보호, 항해·수로·내수로, 안전관리, 해양오염 방제, 선박 검사·인증 등 다양한 업무를 총괄한다.
156) 해양경찰청(2025.3.25.)
157) 위의 자료
158) 위의 자료
159) U.S. Customs and Border Protection, Customs Trade Partnership Against Terrorism (CTPAT)(검색일: 2025.8.14.); U.S. Customs and Border Protection, CSI: Container Security Initiative(검색일: 2025.8.14.)

다. 이민세관단속국(ICE)

미국 이민세관단속국(ICE: US Immigration and Customs Enforcement)는 불법이민, 밀입국, 인신매매, 테러리스트 입국 등을 단속하는 전문기관이다. 해상에서 밀입국 선박, 불법체류 외국인 등이 적발될 시 해안경비대(USCG)와 공조한다. 형사 수사(HSI: Homeland Security Investigations)와 불법 이민자 체포 및 추방(ERO: Enforcement and Removal Operations) 담당 부서가 구분되어 있다. 중남미에서 해양으로 유입되는 인신매매 루트를 단속하거나 공해상에서 문제 선박 적발 시 해안경비대(USCG)와 공동으로 조사를 실시한다.[160]

라. 연방비상관리청(FEMA)

미국 연방비상관리청(FEMA: Federal Emergency Management Agency)은 해양 재난을 담당한다. 연방비상관리청은 국가재난관리체계(NIMS: National Incident Management System)를 가동하여 표준화된 체계와 통제를 해양 재난에도 적용한다.[161] 해양 재난 발생 시 연방비상관리청이 통합재난관리본부가 된다. 해양 재난 발생 시 인력과 장비는 USCG를 통해 구조 업무를 수행한다.[162] 조난이 발생하면 USCG 해상구조조정본부(MRCC: Maritime Rescue Coordination Center)의 수색구조임무조정관(SMC: SAR Mission Coordinator)이 현장지휘관을 지휘 조정한다.[163] 재난의 양태와 장소가 어떠하든지 공통의 용어, 조직 형태, 대응체계가 표준화되어 있다.[164]

160) US Immigration and Custoomos Enforcement(2025.5.28.)(검색일: 2025.8.14.)
161) FEMA(2017). p. 3.
162) FEMA(2016), p. 6.
163) Department of Homeland Security USCG(2013), p.15, 19.
164) United States Coast Guard(2016), pp. 2-16.

(2) 법무부(DOJ)

미국 법무부(DOJ: Department of Justice)는 미국 내 사법 체계 운영의 총괄 기관으로서 범죄 수사, 기소, 재판을 관장하며 연방 수사기관들을 통솔한다. 국토안보부 산하 해안경비대(USCG)가 적발한 해상 범죄(마약, 무기, 인신매매 등)에 대해 기소 및 법적 절차를 총괄한다. 연방수사국, 마약단속국 등 산하 수사기관과의 공조 작전을 지휘한다.[165]

가. 연방수사국(FBI)

연방수사국(FBI: Federal Bureau of Investigation)은 테러 및 연방 범죄 수사를 담당하며, 항만에서 발생하는 테러 위협에 대응한다. 테러 위협에 대한 대응과 예방을 강화하고 테러 사건 발생 시 신속한 대응과 수사를 진행하는 역할을 맡고 있다. 테러 위협 수사를 위해 항만과 관련된 테러 위협 정보를 수집하고 수사한다. 해안경비대(USCG), 세관국경보호청 등과 협력하여 항만보안과 관련된 정보를 공유하고 공동 대응한다.[166]

나. 마약단속국(DEA)

마약단속국(DEA: Drug Enforcement Administration)은 국내외 마약 밀수, 조직범죄, 카르텔 활동을 수사 및 단속한다. 해상 밀수 루트(특히 멕시코·카리브해·태평양 경로)에 대한 작전을 수행한다. 해안경비대(USCG)가 공해상에서 마약 밀수선 적발 시 마약단속국이 정보를 제공하고 수사 및 국제공조를 연계시킨다.[167]

3) 해양 복합위협 대응 거버넌스

해양 복합위협 대응 거버넌스로는 해양작전위협대응프로토콜(MOTR:

165) US Department of Justice(검색일: 2025.8.14.)
166) FBI(2002.8.5.),(검색일: 2025.8.14.); FBI(2025.12.11.)(검색일: 2025.12.11.)
167) DEA Museum(검색일: 2025.8.14.)

Maritime Operational Threat Response)이 있다. 미국에서 해상 위협 발생 시 여러 연방 기관이 신속하게 공조하여 대응하기 위한 정부 간 지휘·운용 프로토콜이다. 9.11 테러 이후 해양보안 체계를 개편하는 일환으로 대통령 지시 사항[168]에 따라 2006년에 도입되었다. 해상에서 발생할 수 있는 테러, 마약 밀수, 무기 운송, 불법 이민, 해상 납치 등 복합적 위협에 대해 사전 정의된 프로토콜에 따라 신속히 공조 대응한다.

국무부, 국방부, 법무부, 상무부, 교통부, 국토안보부 소속의 대표자가 자문그룹(MAG: MORT Advisory Group)으로 참여한다.[169] 2010년 2월에 설립된 글로벌 해양작전위협대응조정센터(GMCC: Global MOTR Coordination Center)를 통해 관련 훈련, 안내, 지원 등 협력 기관을 지원한다.[170]

〈그림 3-1〉 미국 GMCC와 MORT체계



자료: Department of Homeland Security(검색일: 2025.8.14.)

168) US Department of Homeland Security(2004.12.21.)
169) Department of Homeland Security(검색일: 2025.8.14.)
170) 위의 자료

제2절 일본의 해양 복합위협 대상과 대응체계

1. 관리 대상 및 범위

일본은 해양에서의 비군사적·비대칭적 위협을 포괄적으로 인식하고 있다. 제3차 해양기본계획에 따르면 일본이 인식하는 해양위협 유형은 해양이익, 해상교통로, 군사적 수단, 자연재해 등과 관련된다.[171] 해양 이익을 위협하는 것은 영해 침입이다. 외국 관공선의 영해 침입, 외국 군함의 영해 통과, 불법 어업 활동 및 외국 어선의 표류·표착, 외국 조사선의 배타적 경제수역 내 조사 활동, 북한의 탄도미사일 발사·비행 등을 말한다. 해상교통로의 안정성에 대한 위협은 해적과 무장강도, 테러 및 국제범죄 조직, 지역분쟁 등으로 일본계 선박의 안전한 항해와 해상 물류에 지장을 받는 것이다. 군사적 수단은 북한의 탄도미사일 발사 및 일본 상공 통과, 자연재해는 해양에서 발생하는 대형 해양사고와 기상이변을 포함한다. 이러한 위협에 대비하기 위해 일본은 '포괄적 해양안보(Comprehensive Maritime Security)'개념을 통해 영해에서의 국익 강화, 해상교통로의 안정적 운영, 해양의 국제질서 강화를 정책 방향으로 삼고 있다.[172]

복합위협에 대한 일본의 인식은 방위백서에서 나타난다. 2023년 일본 방위백서에 따르면, '하이브리드전(hybrid warfare)'은 군사와 비군사의 경계를 의도적으로 모호하게 만들고, 다양한 비군사적 수단과 군사적 수단을 결합해 상대방의 대응을 복잡하게 만드는 방식이다.[173] 국적을 숨긴 정체불명의 부대를 이용한 작전, 사이버 공격을 통한 통신·중요 인프라 방해,

171) Eifuku(2019), p. 2.
172) Ibid., p. 3.
173) 일본 방위성(2025.4.28.)

인터넷·미디어를 통한 허위 정보 유포 등 다양한 영향력 행사 수단이 복합적으로 사용되는 방식을 하이브리드전으로 간주한다.

2024 일본 방위백서에서 하이브리드전이라는 표현은 러시아-우크라이나 전쟁과 해양영토 분쟁 등에서 언급된다. 러시아에 대해서는 국가에 의한 폭력 사용이 아닌 형태이며 정보전(information warfare)을 포함하고 있다고 표현한다. 일본을 둘러싼 안보 환경에서 영토분쟁을 수반하는 회색지대(Gray Zone) 상황이 지속적으로 발생하고 있으며 군사·비군사 하이브리드전이 더욱 정교하게 사용되고 있다고 명시한다.[174] 2025 일본 방위백서는 일본을 둘러싼 안보 환경에서 해양영토 분쟁을 언급했던 2024년 버전의 문구를 똑같이 언급한다.[175] 따라서 최근 하이브리드전에 대한 일본의 인식은 해양에서 영토분쟁을 수반하는 회색지대 상황에 초점이 있는 것으로 해석된다.

〈표 3-4〉 일본의 해양기본계획과 방위백서에 나타난 위협 분류

유형	내용
해양 이익 침해	영해 침입(관공선, 군함, 어선, 조사선)
해상교통로 안정성	해적과 무장강도, 테러 및 국제범죄 조직, 지역분쟁
군사적 수단	북한의 탄도미사일 발사 및 일본 상공 통과
자연재해	대형 해양사고와 기상이변
하이브리드전	정보전, 영토분쟁을 수반하는 회색지대 상황

자료: Eifuku(2019), pp. 4-6; Ministry of Defense(2023, 2024, 2025) 내용 참고로 저자 작성

174) Ministry of Defense(2024), p. 10, 12.
175) Ministry of Defense(2025), p.15.

2. 관리제도 및 대응체계

1) 주요 법률 및 제도

(1) 해상보안청법

해상보안청법은 해상보안청이 관장하는 사무와 해상보안관의 직무를 규정하는 법이다. 이 법에 따라 해상보안관은 해상 범죄에 대해 형사소송법에 규정하는 사법경찰직원으로서의 직무를 수행한다.[176] 해상보안관에게는 선박의 출입 검사와 서류 제출은 물론 선박의 진행과 출항 정지 등의 강제 권한과 무기사용 권한뿐 아니라 해상 범죄에 대한 수사·체포 권한이 있다.[177] 또한 관세법, 마약 등 단속법령, 어업법, 선원법 등 각 법률에서 정하는 세관 직원, 마약 단속관, 어업 감독관, 선원 노무관 등의 권한도 행사할 수 있다.[178] 해상 범죄에 대해서는 예방 및 진압, 범인 수사 및 구속, 유치 업무, 국제 수사 공조 등을 수행한다.[179]

(2) 국제항해선박 및 국제항만시설의 보안 유지 등에 관한 법률

국제항해선박 및 국제항만시설의 보안 유지 등에 관한 법률(2004)은 해상인명안전협약(SOLAS) 및 국제선박항만보안규칙(ISPS) 개정을 반영하여 제정되었다.[180] 이 법에 따라 해상보안청은 일본 입항 예정 선박에 대한 정보 수집과 추가 조사를 할 수 있다.[181] 입항 24시간 전에 선박 정보를 수집할 수 있으며 선박의 보안 확보 여부가 불확실할 경우 정보를 추가로 요청하거나 인터뷰를 할 수 있다. 선박이 이를 거부할 경우 입항 금지 또는

176) 이순태·이유봉(2017), p. 196.
177) 위의 논문, p. 196.
178) 위의 논문, p. 197.
179) 박경규 외(2023), p. 84.
180) 이순태·이유봉, 앞의 책, pp. 180-195.
181) 함혜현, 앞의 논문, p. 186.

퇴거 명령도 가능하다.

(3) 관세법

관세법은 관세 제정, 수출입 절차, 세금 부과 및 집행을 규정하는 기본 법률이다.[182] 세관 직원은 상급 검찰청 검사총장이 인정할 경우 사법경찰원으로서의 권한을 가지며 무기 휴대 및 사용, 최대 48시간까지 구금 연장 권한을 갖는다. 밀수 의심 화물, 운송수단, 용의자를 압수하거나 검사할 때 경찰관 또는 해상보안관의 협조를 요청할 수 있다(제130조).

(4) 출입국관리 및 난민인정법

출입국관리 및 난민인정법은 외국인의 입국·체류·퇴거를 규정하여 불법 입출국을 방지하는 법률이다.[183] 난민 인정 결정 시 해상보안청장의 의견도 청취하게 되어 있으며(제24조의2) 퇴거 강제 명령 시 입국경비관이 부족할 경우 경찰관 또는 해상보안관이 명령 집행을 대신할 수 있다(제52조). 지역 출입국관리소장 또는 수용소장은 업무 수행을 위해 해상보안청 등 관계 행정기관에 협력을 요청할 수 있고, 요청받은 기관은 원칙적으로 협력해야 한다(제61조의8).

(5) 테러 등 준비죄

조직적 범죄의 처벌 및 범죄수익의 규제 등에 관한 법률은 조직적 범죄 집단이 중대한 범죄를 계획하거나 실행을 준비했을 경우 처벌하는 법률이다.[184] 테러 준비 범죄는 조직적 범죄 집단의 관여, '중대한 범죄'에 대한

182) 일본 법무성(검색일: 2025.8.14.)
183) 일본 법무성(검색일: 2025.8.14.)
184) 일본 법무성(검색일: 2025.8.14.)

계획, 범죄 실행을 위한 준비 행위 등 세 가지 구성 요건을 갖는다. 공모죄 중 테러에 특화된 형태로 2020년 도쿄 올림픽과 국제조직범죄방지협약(UNTOC: United Nations Convention Against Transnational Organized Crime) 가입을 배경으로 제정되었다.[185]

(6) 사이버기본법

사이버기본법(2014)은 일본의 사이버보안 정책을 총체적이고 효율적으로 추진하는 법률이다. 사이버보안전략 수립과 사이버보안전략본부의 설치 및 운영 근거를 마련했다. 2016년 일본연금기구의 정보유출 사건을 계기로 사이버보안전략본부의 사무국인 사이버보안센터(NISC)의 수사 권한과 범위를 확대하도록 개정했다.[186] 2018년에는 2020년 도쿄 올림픽 개최 준비를 위해 다양한 공공·민간 행위자가 정보를 공유하고 조치를 논의하는 사이버보안위원회를 설립하도록 개정했다.[187] 2022년에는 지방자치단체의 법적 책임을 명확히 하고 민관 파트너십 및 정보 공유체제를 구축하도록 개정했다.[188]

2) 기관별 역할

(1) 해상보안청(JCG)

해상보안청(JCG: Japan Coast Guard)은 해상의 치안 확보, 영해 경비, 해난구조, 환경사범 대응 및 해양조사, 해상교통 안전을 관할한다.[189] 해상보안청법에는 해난구조, 해양오염 방지, 선박교통 규제, 수로·항로 표식,

185) 일본대백과전서(검색일: 2025.8.14.)
186) Penta Security(2025.6.11.)(검색일: 2025.8.15.)
187) 위의 자료
188) 위의 자료
189) 박경규 외, 앞의 책, pp. 81-83.

해상안전 확보 등의 업무가 규정되어 있다.[190] 미국 USCG와 달리 항만국 통제는 국토교통성 산하 해사국이 담당한다.

국토교통성 외청으로 공안직과 행정직으로 구성된다. 수사·정보 조직으로서는 해상에서의 범죄 예방 및 진압, 범인 수사 및 체포 등 해상에 한정된 특별사법권만 보유한다.[191] 해상보안청 범죄수사규칙 제2조 제9호에 따르면 해상범죄는 해상에서 "발생"하거나 "시작"되거나 해상에 "영향"을 미치는 범죄이다.[192] 즉, 해상에서 원인 행위가 발생한 사건에 대해 수사권을 가지되 육상(담수 포함)에서 결과 행위가 발생하면 경찰청과 수사를 협력한다.[193] 해상은 현재 해수가 있는 범위를 말하며 하천의 경우 양 끝을 연결한 선을 해상과의 경계로 한다.[194]

해양 복합위협에 대응하는 부서는 경비구난부 내 경비정보과, 국제형사과, 형사과 등이다. 경비정보과는 해상 테러를 소관하고 국제형사과는 경비정보과 소관 해상 테러를 제외한 해적 사건을 담당한다. 국제형사과는 관세, 밀수·밀입국, 난민 등의 국제범죄와 국제공조수사도 담당한다. 형사과는 해양환경과 불법조업 등에 대한 수사를 담당한다. 3관구 소속이지만 본청 국제형사과 지휘를 받는 국제조직범죄대책기지도 있다.[195]

해상보안청 내 해양정보부는 해양공간 관련 정보를 수집하고 관리한다. 해양권익 확보를 위한 영해기선, 대륙붕 등 해저지형 조사와 기상·조류 등의 해양정보 수집, 해도·수로지도 발간, 측량선 운영, 표류예측시스템 개

190) 소관 법령은 해상보안청법 외에도 해상교통안전법, 해상충돌예방법, 해양오염 및 해상재해방지에 관한 법률, 항내해상교통안전법, 항로표지법, 수난구호법, 수로업무법, 배타적 경제수역에서의 어업 등에 관한 주권적 권리 행사 등에 관한 법률 등이 있다. 해양경찰청(2025.3.25.)

191) 위의 자료

192) 박경규 외, 앞의 책, p. 83.

193) 최석윤·최정호(2016), p. 239; 박경규 외, 앞의 책, p. 83.

194) 경찰청과 해상보안청과의 범죄 수사에 관한 협정 해석 및 운용에서의 양해사항 제1조. 박경규 외, 앞의 책, p. 87.

195) 한재진·최정호(2020), p. 97.

발·운영 등을 주요 임무로 한다.[196] 이를 통해 영해, 배타적 경제수역, 대륙붕 등에 대한 해양조사를 직접 실시함으로써 정보 수집과 현장 활동을 유기적으로 연계한다.[197]

(2) 세관

세관은 재무성 산하 관세국 소속으로 수출입 물품 통관 및 관세 부과, 밀수 단속 등을 수행한다. 미국 CBP의 통관 기능과 유사한 업무를 수행한다. 아홉 개의 지역 세관청이 있고 69개 지점, 105개 지사, 아홉 개 경비초소가 있다.[198] 각 세관에는 첩보 관리관이 배치되어 밀수 정보를 수집·분석하고 경찰 또는 해상보안청 등 유관기관과 정보 공유로 범죄에 대응한다.[199]

(3) 출입국재류관리청

출입국재류관리청은 법무성 산하 출입국관리국을 확대·개편하여 2019년에 승격한 기관으로 출입국 심사, 체류 관리, 강제 퇴거 등 전반적인 이민 통제를 담당한다. 한국의 출입국청 기능 및 미국 CBP의 이민 통제 기능과 일부 유사하다. 출입국을 감독하고 정보를 관리하는 총무과와 외국인 정책을 추진하는 정책과, 출입국관리부(입국 심사)와 재류관리지원부(체류 자격 관리, 불법체류 및 밀입국 단속, 난민 인정) 등이 있고 전국 여덟 개 지방출입국재류관리국과 항만·공항 등에 지점이 있다.[200]

196) 해양경찰청(2025.3.25.)
197) 위의 자료
198) 일본 세관(검색일: 2025.8.14.)
199) 일본 세관(검색일: 2025.8.14.)
200) 일본 출입국재류관리청(검색일: 2025.8.14.)

3) 해양 복합위협 대응 거버넌스

일본은 미국의 해양작전위협대응프로토콜(MOTR)과 같은 통합된 프로토콜은 가지고 있지 않은 것으로 보인다. 해상에서 발생하거나 영향을 미치는 위협에 대해서는 해상보안청에 일임하여 일원화하고 있기 때문이다. 앞서 살펴보았듯이 해상에서 시작된 위협이 담수를 포함하여 육상으로 진입할 경우 경찰에 협조 및 인계하는 절차를 가지고 있다. 일본의 해양 복합위협 대응 거버넌스는 종합해양정책본부 설치법(2007)에 따른 해양기본법과 해양기본계획에서 유추해 볼 수 있다. 이 법과 계획에 따라 관계 행정기관이 정책을 조정하고 있고 해양종합정책본부 회의가 개최되고 있다.[201]

제3절 영국의 해양 복합위협 대상과 대응체계

1. 관리 대상 및 범위

영국은 해양영역(maritime domain)이 복잡하고 다양한 부문과 행위자로 구성되어 있다는 인식 아래 '정부 전체적 접근(whole-of-government approach)'을 지향한다.[202] 해양안보 측면에서는 테러리즘과 극단주의, 불안정성, 규범 기반 국제질서의 붕괴, 사이버위협과 폭넓은 기술 발전, 심각하고 조직화된 범죄, 질병과 자연재해 등에 주목하고 있다.

영국의 해양안보국가전략(Nartional Strategy for Maritime Security) 2022는 안보 대상을 '국경', '항만', '자유항(Freeports)'[203], '사이버'로

201) 일본 해양종합정책본부(검색일: 2025.8.14.)
202) Department for Transport(2019)

구분한다.[204] 국가위험등록부(National Risk Register) 2025는 "공공장소 테러 공격"의 하위 유형으로 영국 수역 내 혹은 인근에서 선박이 공격당하는 악의적인 해사사고(malicious maritime incident)를 명시했다.[205]

영국 교통부가 발간한 자료(Maritime 2050: Navigating the Future)에 따르면 해양안보에서 다루는 영역은 '수역', '항만과 선박', '글로벌 해운 항로', '사이버', '테러', '해양 범죄(밀수, 인신매매 등)와 해적' 등이다.[206]

〈표 3-5〉 영국 교통부의 해양위협 분류

유형	내용
수역	해양영역인식(MDA)을 통한 본토 및 해외영토 위협 인식
항만과 선박	침수 대응, 항만보안, 화물과 승객 검사
글로벌 해운 항로	국제해양규범(UNCLOS) 위반, 자유항행권 침해
사이버	해운·항만 시스템 해킹
테러	드론 등 첨단 기술 활용, 해운 및 항만 표적
해양 범죄와 해적	밀수, 무기거래, 인신매매

자료: Department for Transport(2019) 내용 참고로 저자 작성

수역에 대해서는 국가 행위자에 의한 잠재적 위협을 발견하고 또 발견하는 능력을 배양하는 데 중점을 두고 있다. 이를 위한 해양영역인식(MDA)과 유관기관의 협력, 해외영토의 항만보안 규제당국, NATO와 유럽 동맹국 등을 주요 파트너로 한다. 영국은 본토뿐 아니라 영국의 주권이 미치는 14개 해외영토가 있고 세계에서 다섯 번째로 넓은 EEZ를 가지고 있다.[207]

203) 기존 자유무역항은 주로 항만지역에서 무역·환적 중심으로 특정 지역의 경제 발전을 목표한다. 영국의 자유항은 항만 + 내륙 산업·물류단지에서 무역+제조·신산업 투자 유치를 중심으로 브렉시트 이후 경제 회복과 글로벌 무역 허브 구축을 목표로 한다. 항만, 배후산업단지, 물류허브를 묶은 종합 경제특구 형태로 더 넓은 범위의 세제 혜택과 규제 완화를 제공한다. 자세한 내용은 HM Treasury(2020) 참고
204) HM Government(2022)
205) HM Government(2025), p. 33, 54.
206) Department for Transport, op. cit.
207) Department for Transport, op. cit.

이처럼 광범위한 해양영역으로 인해 관련 작전은 첩보에 기반한다.

항만과 선박에 대해서는 섬 국가로서 동부 해안 폭풍 해일에 의한 홍수와 극한 기후에 따른 항만 침수, 국제선박항만보안규칙(ISPS)의 집행, 해양산업과 무역 보호를 위한 해적 위협 대응, 항만·선박 운영의 자동화 시스템에 따른 사이버위협 등에 주목하고 있다.

글로벌 해운 항로에 대해서는 기니만의 범죄, 술루·셀레베스해의 테러, 남·동중국해의 긴장, 북극항로를 비롯해 전략적 에너지 초크포인트(chokepoint)인 호르무즈 해협과 홍해-아덴만을 연결하는 바브엘만데브 해협(Bab-el-Mandeb Strait) 등에 주목한다.

사이버위협은 2017년 세계 최대 컨테이너 운송 기업인 머스크(Maersk)사를 해킹한 NotPetya 랜섬웨어가 대표적이다.[208] 전 세계 76개 항만 터미널이 운영을 중단하고, 그로 인해 약 2억~3억 달러의 피해가 발생한 것으로 보고된다.[209] 영국 교통부는 사이버보안팀을 창설하고 영국 정보통신부 산하 국가사이버보안센터(NCSC: National Cyber Security Centre)와 긴밀히 협력하고 있다.

2. 관리제도 및 대응체계

1) 주요 법률 및 제도

(1) 해양항해법

해양항해법(Marine Navigation Act 2013)은 기존 법률을 개정하여 항행과 항만 운영, 항만경찰, 등대당국, 선박의 인력배분 등에 관한 규칙

208) Ibid., p. 277.
209) Ibid., p. 277.

을 개선했다.[210] 지정된 항만 당국이 항만 내 또는 진입·진출 선박에 대해 항만지시(Harbour Directions)를 발령할 수 있고, 특정 조건하에서는 항만 당국의 조종 권한을 해제할 수도 있다. 항만경찰(Port Constables)은 체포·수색·법집행 권한을 가진다. 원래 법적 권한은 항만 및 주변 1마일 이내였지만 해당 지역 경찰청장의 동의하에 항만 밖(지역 경찰 구역 전체로 확대)에서도 업무를 수행하거나 항만 내 범죄에 대해 체포할 수 있게 한다.

(2) 관세 및 세관 관리법

관세 및 세관 관리법(Customs and Excise Management Act 1979)은 밀수 행위에 대해 세관 당국이 조치를 취하는 법적 근거를 제공한다.[211] 밀수 방지를 위해 선박을 정박시키거나 인양할 수 있고 밀수 방지에 정당하게 관여하기 위해 자유로운 순찰과 통과를 할 수 있게 한다.

(3) 불법이민법

불법이민법(Illegal Migration Act 2023)은 영국으로의 무단 입국, 특히 소형 보트를 이용한 밀입국(small boat crossings)을 줄이기 위한 법률적 수단이라는 점을 입법 목적에 포함한다.[212] 밀입국자는 구금 및 추방하고 다시 입국하지 못하도록 조치한다.

(4) 대테러·국경안보법

대테러·국경안보법(Counter-Terrorism and Border Security Act 2019)은 항만 및 국경 통제 시 적대적 활동에 연루 가능성이 있는 사람을

210) 영국 법령 포털(검색일: 2025.8.14.)
211) 영국 법령 포털(검색일: 2025.8.15.)
212) 영국 법령 포털(검색일: 2025.8.16.)

정지·질문·구금할 수 있는 법적 근거를 제공한다.[213] 적대적 활동은 공격, 스파이 활동, 국가 기반 위협 등 넓은 개념으로 마약 밀수, 무기 반입 등 국제범죄 연계 가능성을 염두에 두고 있다.

(5) 국가안보법

국가안보법(National Security Act 2023)은 간첩, 사보타주, 외국 세력의 간섭 및 재정적 이득 등 국가 안보 전반에 대한 대응을 목적으로 한다. 사보타주는 해커 공격을 포함해 물리적·디지털 방식의 파괴 행위를 포괄한다.[214]

(6) 국경안보·망명·이주법

국경안보·망명·이주법(Border Security, Asylum and Immigration Bill)은 2025년 5월 현재 입법 영향 평가 중이다.[215] 영국의 국경 안보에서 최대 현안은 조직 이민 범죄이다. 2020년 이후 비정규 도착자의 주요 입국이 소형 보트를 통해 이루어졌고 2024년의 경우 81%에 달했다. 이 법은 심각하고 조직적인 범죄에 연루된 것으로 의심되는 사람에게 더 빨리 개입할 수 있게 한다. 해상으로 영국을 여행하는 동안 다른 사람에게 심각한 부상이나 사망을 초래할 위험이 있는 방식으로 행동하는 개인에 대해 조치할 수도 있다.

(7) 사이버보안·복원법

사이버보안·복원법(Cyber Security and Resilience Bill)은 네트워크·정보시스템보안규정(Network and Information Systems(NIS) Regulation

213) Home Office(2020)
214) 영국 정부, National Security Act Factsheet(검색일: 2025.8.15.)
215) 영국 정부, Impact assessment, Border Security, Asylum and Immigration Bill 2025: overarching impact assessment(검색일: 2025.8.15.)

2018)[216]을 현대화하는 법안으로 2025년 내 의회 제출을 앞두고 있다.[217] 필수 서비스 제공자뿐 아니라 데이터 센터 운영자 등 공급망 전반으로 규제 범위 확대, 규제 기관의 권한 강화, 사고 보고 체계 강화, 국가 차원의 복원력 확보 전략 등을 포함한다.

2) 기관별 역할

(1) 교통부

영국에서는 교통부 산하 '항공·해양 및 보안 차관(Aviation, Maritime and Security Minister)'이 항공 및 해양 부문을 총괄하고 해양경비청(MCA)과 민간항공청(CAA: Civil Aviation Authority)이 보안과 비상사태, 국제교통정책을 책임진다.[218]

가. 해양경비청(MCA)

영국 해양경비청(MCA: Maritime and Coastguard Agency)은 교통부의 외청이다. 해양경비청은 선박과 선원의 자격에 대한 법령과 지침을 제공하고 선박 안전, 보안, 해양오염 예방, 선원의 건강·안전·복지 등을 전담한다.[219]

해양경비청의 지역 사무소 역할을 하는 해양사무소(Marine Office)가 영국 전역에 분포해 있다. 해양사무소는 선박 등록 검토, 선박 안전 검사와 인증, 항만국 통제, 해기사 면허 및 승선 기준 확인 등의 업무를 한다.[220]

216) 사이버보안 관련 최초의 범유럽 차원의 법령으로 EU가 2016년에 제정한 네트워크·정보시스템보안지침(Network and Information Systems(NIS) Directive)를 이행하기 위한 규정
217) 영국 정부, Cyber Security And Resilience Bill(검색일: 2025.8.15.)
218) 영국 정부(검색일: 2025.4.28.)
219) MCA(검색일: 2025.4.25.)
220) 영국 정부(검색일: 2025.4.29.)

나. 해안경비대(HMCG)

해안경비대(HMCG: His Majesty's Coastguard)는 해안경비청 산하에 있다. 해안경비대(HMCG)는 해양 보안뿐 아니라 수색구조, 해상교통 관제, 해양오염 방제, 잔해 수거, 해양 재난 대응, 국제협력 등을 담당한다.[221] 해상 수색과 구조, 위험 선박 모니터링, AIS 감시 등을 통해 밀입국과 사고 대응에 관여한다.

해양경비청과 해안경비대(HMCG)는 안전과 환경 측면의 감시 기관으로 형사 수사권은 없다. 의심 선박 정보나 해양오염 증거, AIS 조작이나 불법 등록 선박, 선박의 세금 회피나 불법행위 등에 관한 정보를 제공하고 통보하는 식으로 다른 기관과 공조한다. 즉, 수사기관에 정보를 제공하는 방식으로 공조 체계에 참여한다.

(2) 내무부

가. 국경수비대(Border Force)

영국에서 해상으로부터 유입되는 입국자를 심사하고 선박을 검색하며 마약·무기 밀수를 단속하는 것은 내무부 소속의 국경수비대(Border Force)이다. 항만·공항·해상에서의 출입국 통제, 화물 검색, 선박 검문을 할 수 있다. 수사권과 현장 단속권(증거 확보 권한)을 일부 보유하고 있으나 조직 추적이나 범죄 수사를 하는 형사 수사권은 없다.

나. 국가범죄청(NCA)

해양에서 일어나는 범죄에 대한 실질적인 수사권은 국가범죄청(NCA: National Crime Agency)이 가지고 있다. 국가범죄청은 마약·무기 밀수, 밀입국, 테러 등을 연계 수사하고 정보를 분석하며 국제수사협력도 담당한

221) HMCG(검색일: 2025.4.25.)

다. 해상 감시 자산은 없지만 해양경비청(해안경비대(HMCG)) 등으로부터 정보를 공유받는다.

(3) 세관 및 국세청(HMRC)

영국에는 재무부 산하에 관세청과 국세청이 통합된 세관 및 국세청(HMRC: His Majesty Revenue and Customs)이 있다. 세관 단속, 불법 물품 적발, 밀수 추적 등을 담당한다. 선박을 통한 탈세, 세금 회피, 불법 무역에 대한 수사 권한을 보유하고 있다.

3) 해양 복합위협 대응 거버넌스

해양 복합위협 대응 거버넌스로는 합동해양안보센터(JMSC: Joint Maritime Security Centre)가 있다. 영국의 해양안보 사건에 대응하는 다부처 조직이다. 영국의 해양영역인식을 유지하고 안보, 법과 질서, 해양 환경 위협에 대응하는 범정부 협력체계이다. 2010년부터 영국의 민·군 간 첩보, 데이터, 역량을 결합해 온 국가해양정보센터(NMIC: National Maritime Information Centre)를 통합하여 국내외의 작전 영향력을 극대화시켰다.[222]

JMSC의 합동해양작전조정센터(JMOOC: Joint Maritime Operations Coordination Centre)는 최첨단 기술을 활용해 영국 수역에 대한 24시간 모니터링을 제공한다. 국경수비대, 해군(RN: Royal Navy), 국방부 등이 이끌고 대테러 경찰, 교통부, 외무부, 내무부, 해안경비대(HMCG), 세관 및 국세청(HMRC), 국가범죄청(NCA), 해양관리기구(MMO), 스코틀랜드 해양청(Marine Scotland)이 지원한다.[223]

222) JMSC(검색일: 2025.4.25.)
223) JMSC(검색일: 2025.4.25.)

제4절 국제 비교 분석 및 국내 적용 시사점

1. 국가별 특징 및 대응체계 비교

1) 국가별 요약 및 특징

미국의 국토안보부는 공공안전과 보안, 국경과 이주, 기반시설, 경제 부문을 주요 안보 위협 대상으로 보고 있다. 해양에서 발생하는 위협 주요 위협 유형은 마약·무기, 불법 이민·납치·해적, 불응 선박, 항만 테러 등이 있다. 주요 법제 대상은 9.11테러 이후 선박과 항만에 대한 물리적 보안에 역점을 두다가 컨테이너, 세관, 외국 항만과 국제 공급망, 국제 해상화물, 해양테러, 사이버 사건 등으로 확장되었다. 대응체계는 국토안보부 산하의 해안경비대(USCG)를 중심으로 세관국경보호청, 이민세관단속국, 연방비상관리청이 협력하여 물자, 사람, 재난 등의 유형별 위협에 유기적으로 통합 대응한다. 법무부 산하의 연방수사국과 마약단속국은 테러와 마약 등 조직범죄 대응에 협력한다. 해양작전위협대응프로토콜(MOTR)을 통해 해양 복합위협 대응 거버넌스를 구축하고 있다.

일본은 해양 이익, 해상교통로, 군사적 수단, 자연재해 등을 해양위협으로 인식하고 있다. 복합위협에 대해서는 해양에서 영토분쟁을 수반하는 회색지대 상황에 초점을 두고 있다. 주요 법제는 해상보안청법, 국제항해선박항만법, 관세법, 출입국 관련법, 테러 관련법, 사이버기본법 등이 있다. 미국처럼 사이버위협 대응을 관장하는 독립된 단일법이나 해양 사이버위협을 다루는 하위법령은 따로 두지 않는 것으로 보인다. 대응 기관은 해상보안청으로 일원화되어 있다. 국토교통성 산하 해사국이 담당하는 항만국 통제를 제외하면 해상보안청이 해역에서 발생하거나 시작되거나 영향을 미치는 모든 범죄를 관할한다. 출입국재류관리청과 세관이 물자와 사람에 대한 행

정 단속을 맡는다.

영국의 해양안보는 국경, 항만, 자유항, 사이버를 주요 대상으로 한다. 수역, 항만과 선박, 글로벌 해운 항로에서 발생하는 해양 범죄와 해적, 테러, 사이버위협 등을 주요 위협으로 고려하고 있다. 주요 법제는 해양항해법, 관세법, 망명·이민·이주 관련 법, 안보·테러 관련법, 사이버보안·복원법(법안 제출 예정) 등이 있다. 대응체계는 유관기관의 역할이 제도적으로 결합되어 있다. 해양경비청(정보 입수)-국경수비대(검문·단속)-국가범죄청(수사) 순으로 역할이 맞물려 있으며 물자에 대해서는 세관 및 국세청, 형사 고발에 대해서는 검찰기소청으로 인계한다. 해양 복합위협 대응 거버넌스로는 합동해양안보센터와 합동해양작전조정센터 등이 있다.

미국, 일본, 영국은 국가별 환경에 따라 해양에서 발생하는 위협에 대한 인식이 각이하다. 또한 각국의 제도·문화적 환경에 따라 법제와 대응체계에 특징이 있다. 미국은 9.11테러를 기점으로 국토 안보 위협에 대한 경각심을 가지고 해양경비, 출입 물자와 사람, 재해 등을 통합하는 단일 부서인 국토안보부 중심으로 대응한다. 일본과 영국은 섬 국가라는 공통점이 있지만 대응체계는 서로 다르다. 일본은 해양 이익과 군사 위협에 초점을 두고 있다. 해상보안청이 해양조사까지 맡아 해양 권익 확보를 위한 역량을 집결하고 있다. 미국 및 영국과 달리 사이버위협에 대응하는 독립된 단일법이 없다는 점도 특징이다. 영국은 해양 복합위협의 주요 대상과 통로가 되는 항만·선박 관리는 해양경비청에, 현장 1차 대응은 국경수비대에 분리되어 있다. 해양경비청과 국경수비대가 수사기관이라기보다는 행정·단속기관이라는 점도 특징이다.

〈표 3-6〉 미국·일본·영국의 해양 복합위협 대응체계 요약

구분	미국	일본	영국
해양위협 인식	• 공공안전 • 국경과 이주 • 주요 기반시설 • 경제 안보	• 해양 이익 • 해상교통로 • 군사적 위협 • 자연재해 • 하이브리드전	• 수역 • 항만과 선박 • 글로벌 해운 항로 • 사이버 • 테러 • 해양 범죄와 해적
주요 법률	• 해양운송법 • 항만보안법 • USA Freedom Act • Tariff Act of 1930 • Immigration and Nationality Act • Homeland Security Act of 2022 • National Cybersecurity Protection Act 2014	• 해상보안청법 • 국제항해선박항만법 • 관세법 • 출입국관리 및 난민인정법 • 테러 등 준비죄 • 사이버기본법	• 해양항해법 • 관세 및 세관 관리법 • 불법이민법 • 대테러·국경안보법 • 국가안보법 • 국경안보·망명·이주법 • 사이버보안·복원법
주요 대응 기관	• 해안경비대(USCG) • 세관국경보호청 • 이민세관단속국	• 해상보안청 • 세관 • 출입국재류청	• 해양경비청 • 국경수비대 • 세관 및 국세청 • 국가범죄청
통합 거버넌스	• 해양작전위협대응프로토콜(MOTR)	–	• 합동해양안보센터(JMSC)

자료: 저자 작성

2) 국가별 대응체계 비교

미국은 해안경비대(USCG)를 비롯해 세관국경보호청·이민세관단속국을 산하에 둔 국토안보부 중심이다. 일본은 해상보안청이 대부분을 전담하고, 출입국재류관리청, 세관이 연계된다. 영국은 해양경비청, 국경수비대, 세관 및 국세청, 국가범죄청 등 기능별로 분화되어 있다. 즉, 미국은 유관기관

간의 역할이 매우 유기적으로 통합되어 있다. 영국은 미국보다는 느슨한 형태로 다기관에 기능이 분산된 대신 제도적으로 결합된다. 일본은 명확한 권한을 명시함으로써 실행 권력을 중심으로 대응체계가 일원화되어 있다.

국가별 해양 복합위협에 대응하는 체계의 최전선에는 우리나라 해양경찰청에 상응하는 해양 경비·치안 기관이 있다. 국가별 1차 대응 기관의 역할을 중심으로 비교하면 다음과 같다.

미국 해안경비대(USCG)는 국토안보부 소속이지만, 전시에는 해군 소속으로 전환되는 이중지휘체계를 보유하고 있다. 해상 치안, 환경, 운송, 구조, 방위 등 해양 관련 거의 모든 기능을 수행하는 준군사조직이다. 해안경비대(USCG)는 해상에서 범죄를 직접 수사할 수 있다. 때에 따라 마약단속국, 이민세관단속국 등과 합동 수사한 후 검찰에 송치한다. 세관국경보호청은 항만에서 밀수 사건이 적발될 시 초동 수사를 한다. 항만에서 밀수품·밀입국자 발견 시 압수·체포하여 마약단속국, 이민세관단속국 등에 이첩한다. 이민세관단속국은 연방 수사기관으로서 조직적·국제적 차원의 본격 수사를 주도한다. 밀입국 조직·국제 밀수 네트워크를 수사하여 증거 및 피의자를 확보하는 등 수사 범위가 넓은 편이다. 즉, 미국의 해양 복합위협 대응체계에서 1차 대응 기관인 해안경비대(USCG)와 세관국경보호청은 해상과 국경에 국한해 수사권을 갖고 이민세관단속국은 국내 유통이나 조직범죄까지 직접 수사할 수 있다.

일본 해상보안청(JCG)은 국토교통성 소속이지만, 사법경찰권·강제권을 보유하고 단속, 수사, 구조, 환경 대응까지 일원화되어 실행력이 높다. 군사적 상황 시 해상자위대와 임무를 분리하고 필요시 공조한다. 미국의 해안경비대(USCG)와 마찬가지로 수사권, 체포권, 압수권을 갖고 활동 범위가 해상에 국한된다. 출입국재류관리청은 불법 입국·체류에 관해, 세관은 밀수에 관해 제한된 수사·체포 권한을 갖는다. 일본의 해양 복합위협 대응체계에서도 1차 대응 기관인 해상보안청을 비롯해 출입국재류관리청과 세

관이 관할 업무에 제한된 수사권을 가지고 그 범위는 해상과 국경에 국한된다. 내륙에 연계된 마약·무기 밀수나 조직범죄 사건은 경찰에 이첩한다.

영국 해안경비대(HMCG)는 교통부 산하 해양경비청(MCA) 소속으로 구조·통신에 집중한다. 해양 치안·단속은 국경수비대가 주도한다. 영국의 경우, 국경수비대와 해양경비청 모두 수사권이 없는 것이 특징이다. 국경수비대는 이민·관세 차원의 검문·체포·압수를 제한적으로 집행할 수 있지만 수사는 할 수 없다. 해양경비청도 미국 해안경비대(USCG)나 일본 해상보안청과 같은 해상 범죄 수사권이 없다. 즉, 영국의 국경수비대와 해양경비청은 행정적 단속·체포 권한만 갖는다.

〈표 3-7〉 국가별 해양 복합위협 1차 대응 기관 권한 비교

구분	단속	체포	수사 (해상 적발)	수사 (내륙 연계)
한국	해양경찰청			
미국	해안경비대(USCG)			이민세관단속국
일본	해상보안청			경찰
영국	국경수비대		국가범죄청	

자료: 저자 작성

〈표 3-8〉 국가별 해양 복합위협 대응체계

구분	한국	미국	일본	영국
1차 대응	해양경찰청	해안경비대 (USCG)	해상보안청	국경수비대
항만국 통제	해양수산부 (항만보안공사)	해안경비대 (USCG)	국토교통성	해양경비청
밀입(출)국 → 수사	출입국 관리사무소 → 해양경찰청	이민세관단속국	출입국 재류관리청 →경찰	국경수비대 → 국가범죄청
밀수(출)입 → 수사	관세청 → 해양경찰청	세관국경보호청 → 마약단속국/이민세관단속국	세관 →경찰	국경수비대 /세관 및 국세청 → 국가범죄청

자료: 저자 작성

2. 실효적 대응방안 시사점

미국, 일본, 영국 등 국외 사례는 세 가지 형태의 해양 복합위협 대응체계와 체계별 필요 사항에 대해 다음과 같은 시사점을 준다.

첫째, 단일 부처 내에 해양경비를 비롯해 밀입(출)국, 밀수(출)입 등 해양 국제범죄 관련 부서가 통합된 형태이다. 미국의 해양 복합위협 대응체계가 이에 해당한다. 국토안보 관점에서 해양안보에 위협을 야기하는 요소를 통합적으로 관리한다. 해양경비 전담기관(해안경비대(USCG))은 '정보 수집'부터 '단속·체포'는 물론 '형사 수사'까지 할 수 있다. 위협 요소를 포착할 시 직접 조사하고 적발하는 장점이 있다. 관세 및 이민 전담기관이 해양경비 전담기관과 같은 부처에 소속되어 있으므로 효율적인 권한 집행도 기대된다. 관세 전담기관(세관국경보호청)의 권한 집행 구역은 항만 등으로 제한되지만 이민 전담기관(이민세관단속국)은 내륙 연계 수사가 가능하다. 따라서 해양에서 유입되는 위협을 육상에서도 추적할 수 있다. 유관기관이 공동 대응하는 시스템이 유기적으로 연결되어 있어 해양 복합위협에 가장 효과적으로 대처할 수 있는 형태로 보인다.

미국식 해양 복합위협 대응체계는 ① 유관기관 대부분이 동일 부처에 소속되어 있고, ② 형사 수사는 해상 적발 단계에서 내륙 연계 단계로 이어질 수 있어야 한다.

둘째, 유관기관의 소속과 역할이 분리되어 있지만 해양경비 전담기관에 권한이 집중된 형태이다. 일본의 해양 복합위협 대응체계가 이에 해당한다. 해양경비 전담기관(해상보안청)은 '정보 수집'부터 '단속·체포'는 물론 '형사 수사'까지 할 수 있지만 활동 범위가 '해상'에 국한된다. 위협 요소를 포착할 시 직접 조사하고 적발하지만, 그 범위가 '해상'을 벗어나면 육상 경찰에 이첩한다. 관세 및 이민 전담기관(세관·출입국재류관리청)의 권한

집행 구역도 항만 등으로 제한된다. 따라서 해양에서 유입되는 위협을 단일 기관이 집중적으로 관리하는 대신, 권한 집행의 구역을 명시하여 육상과 분리한다. 해양 복합위협이 발생하는 '초기 단계'에 효과적으로 대처할 수 있는 형태로 보인다.

일본식 해양 복합위협 대응체계는 ① 해양경비 전담기관에 대부분의 권한이 집중된 대신, ② 형사 수사 권한은 해상 적발 단계와 내륙 연계 단계를 명확히 구분한다.

셋째, 유관기관의 역할이 더 세부적으로 분리되어 있지만 제도적으로 결합이 잘 되어 있는 형태이다. 영국의 해양 복합위협 대응체계가 이에 해당한다. 해양 복합위협에 대한 '정보 수집', '단속·체포', '형사 수사' 권한을 가진 기관이 모두 다르다. 해양 전담기관(해양경비청)이 정보를 수집해 경비 전담기관(국경수비대)에 전달하고, 경비 전담기관이 단속·체포한 사건을 수사 전담기관(국가범죄청)에 이첩한다. 해양 복합위협 사건 발생 시 유관기관이 손에 손을 잡고 이어달리기하는 형태이다. 관세 전담기관(세관 및 국세청)도 관여하기는 하지만 경비 전담기관이 관세 및 이민 업무까지 연계하여 수행하는 것이 장점이다. 경비-관세-이민 업무가 유기적으로 연결되어 있어 해양 복합위협 유입에 가장 효율적으로 대처할 수 있는 형태로 보인다.

영국식 해양 복합위협 대응체계는 ① 유관기관의 역할이 정보 수집, 단속·체포, 형사 수사 등으로 단계별 세분화된 대신 ② 유관업무인 경비-관세-이민(경비 전담), 해상-육상 수사(수사 전담)가 각 전담기관에 집중된다.

미국식 해양 복합위협 대응체계처럼 유기적 통합이 가장 효과적이겠지만 이처럼 유관기관을 하나로 통합하기는 쉽지 않다. 법·행정적으로 여러 변화와 정무적 의견수렴이 필요하기 때문이다. 따라서 일본식 또는 영국식 해양 복합위협 대응체계가 현실적인 대안으로 고려된다.

일본식 해양 복합위협 대응체계 마련을 위해서는 해양경비 전담기관을 중심으로 해양 국제범죄 관련 업무를 일원화하는 대신 해상-육상 수사의 권한을 분리·명시하는 것이 필요하다.

영국식 해양 복합위협 대응체계 마련을 위해서는 경비 전담기관에 관세·이민 관련 업무 집행 기능을 강화하고 수사 전담기관에 해상-육상 수사의 권한을 연결시키는 것이 필요하다.

04
해양 복합위협 국내 대응체계와 데이터 분석

본 장에서는 앞 장에서 제시된 해양 복합위협에 대한 유형별 국내 대응체계를 심층적으로 검토한다. 구체적으로 각 위협 유형에 따라 우리나라가 마련한 대응체계의 구조와 운용 현황을 분석하고, 위협이 발생하는 위치별로 국내 체제가 실제로 적절하게 구축되어 있는지 점검한다. 이어서 위협별 위험성을 체계적으로 분석해 국내 해양 복합위협의 유형별 우선순위를 도출하고, 이를 바탕으로 현행 대응체계의 미비점과 정책적으로 개선이 요구되는 사항을 제시하며, 효과적이고 실질적인 위협 대응을 위한 정책 방향성을 제시한다.

제1절 해양 복합위협 국내 대응체계

해양 복합위협은 앞에서 검토한 바와 같이 해양 국제범죄, 해양테러, 해양 사이버위협의 세 가지로 크게 유형화할 수 있다. 이에 본 절에서는 개별 유형의 위협들에 대한 국내 대응체계를 먼저 검토한다. 다만, 최근 해양 복합위협의 경향은 앞에서 살펴본 바와 같이 개별 유형에 한정하여 발생하기

보다, 사이버수단을 이용한 테러 행위 내지 물리적 위협을 일으키는 복합적인 형태로 나타난다. 이에 본 절에서는 개별 유형에 따른 국내 대응체계를 검토한 후, 개별 유형의 위협이 동시다발적으로 나타날 경우 국내 관련 제도가 효과적으로 운용되기 위한 정책적 시사점을 도출한다.

1. 해양 국제범죄 국내 대응체계

1) 해양 국제범죄 유형별 대응체계

앞에서 검토한 바와 같이 해양 복합위협 중 해양 국제범죄의 유형은 밀입(출)국, 밀수(출)입, 납치 및 인신매매, 해적 및 무장강도, 불법조업, 해양오염을 포함한 기타 국제범죄로 구분할 수 있다. 그리고 이러한 국제범죄의 종류는 해양경찰청에서 관리하고 있는 목록을 기준으로 〈표 4-1〉과 같이 구분할 수 있다.

〈표 4-1〉 해양 국제범죄 유형, 범죄 종류 및 근거 법령

유형	범죄 종류	근거 법령
밀입(출)국	밀입국	출입국관리법 등
	무사증	제주특별법 등
	무단이탈	출입국관리법 등
	밀항	밀항단속법 등
	밀출국	출입국관리법 등
	불법체류, 취업	선박입출항법, 선박직원법, 선원법, 직업안정법, 출입국 관리법 등
밀수(출)입	밀수입	관세법, 담배사업법, 상표법, 식품위생법, 야생생물법, 약사법, 총포화약법, 축산물위생관리법, 특정범죄가중법 등
	밀수출	농수산물품질관리법
	마약류 범죄	마약류관리법

유형	범죄 종류	근거 법령
	해양산업기술 유출	산업기술보호법, 부정경쟁방지법 등
	지적재산 침해	상표법 등
	불법위폐, 외국환거래	외국환거래법, 특정경제범죄법 등
납치 및 인신매매	납치 및 인신매매	형사법
해적 및 무장강도	인권침해	형사법
	외국인권익침해	외국인고용법, 직업안정법
불법조업	불법조업	영해 및 접속수역법, 경제수역어업주권법 등
해양오염 등 기타	외국선박 환경오염	항만대기질법, 해양환경관리법
	기타	검역법, 선박법, 선박안전법 등

자료: 한국해양수산개발원(2025.5.12.) 참조하여 저자 작성

(1) 밀입(출)국 및 밀수(출)입

해양 국제범죄는 다양한 법령에 따라 여러 기관이 그 관할 및 대상에 따라 대응하고 있다. 밀입(출)국의 경우, 항만에서 출입국·외국인청이 주로 대응하고 있다. 특히, 「출입국관리법」에 따라 선박 등은 출입국항에 출·입항할 때 출입국관리공무원의 검색을 받아야 한다.[224] 선박 등이 부득이하게 출입국항이 아닌 장소에 출·입항하여야 할 경우, 출·입항 예정통보서를 작성하여 미연에 지방출입국·외국인관서에 제출하고 선박 검색을 받아야 한다.[225] 밀수(출)입의 경우, 관세청이 항만 등에서 「관세법」 등 관련 법에 따라 주로 대응하고 있다. 특히, 국제항해선박은 관세법에 따른 국제항에 출·입항할 경우 허가를 받아야 하며, 국제항에 입항 시 수출입 금지 물품 확인을 위해 선박용품, 여객 및 승무원 명부, 승무원 휴대품목록, 적재화물목록을 보고하고 출항 시에는 적재화물목록을 제출해야 한다.[226] 더불어 관세청은 필요하다고 인정될 경우, 밀수가 의심되는 선박에 대해, 해군, 해

224) 출입국관리법 제69조 제1항
225) 출입국관리법 제69조 제2항
226) 관세법 제134조-제136조, 제234조; 관세법 시행령 제157조 등

양경찰청에 협조를 요청하여 추적감시 또는 정선 명령을 실시하고 검문·검색 또한 실시할 수 있다.[227] 또한 마약 밀수 등과 관련해서는 「마약류관리법」에 따라 식품의약품안전처에 설치된 마약류대책협의회가 관리 및 대응하고 있으며, 특히 마약류 해상 유통 및 밀수에 대해서는 해양경찰청과 관세청이 단속을 실시한다.

〈그림 4-1〉 마약류대책협의회 기능 및 기관별 역할



자료: 식품의약품안전처(검색일: 2025.9.9.); 마약류관리법 제2조의4를 참조하여 저자 편집

국제항 등 무역항을 제외한 일반 연안 및 해상에서의 밀입(출)국, 밀수(출)입을 단속하는 것은 해양경찰청이 담당한다. 해양경찰청은 일반사법경찰로서 해상을 통해 국내로 유입되는 밀입국자들을 「출입국관리법」에 따라 해상에서 단속하거나 검거하는 역할을 담당한다. 또한, 해양경찰청은 우리나라 국민이 적법한 절차를 취하지 아니하고 국외로 도항(渡航)하는 것을

227) 관세법 제287조의2

방지하기 위해 「밀항단속법」을 제정하고 공해상에서 환승하여 도주하거나 중고 수출선박을 이용하여 밀항하는 사람들을 직접 단속 및 대응한다.[228] 또한 해양경찰은 밀수와 관련하여 관세청의 협조 요청에 따라 해상에서의 의심 선박 등에 대해 단속 및 검색을 실시한다. 특히, 선박 또는 해상을 통한 마약 유통과 관련해서는 마약류대책협의회 위원으로서 해양경찰청이 직접 단속 및 검거하기도 한다.

〈표 4-2〉 해양 국제범죄 유형별 대응 기관(밀입(출)국, 밀수(출)입)

유형	범죄 종류	근거 법령	대응 기관
밀입(출)국	밀입국	출입국관리법 등	출입국·외국인청 해양경찰청
	무사증	제주특별법 등	
	무단이탈	출입국관리법 등	
	밀항	밀항단속법 등	
	밀출국	출입국관리법 등	
	불법체류, 취업	선박입출항법, 선박직원법, 선원법, 직업안정법, 출입국 관리법 등	
밀수(출)입	밀수입	관세법, 담배사업법, 상표법, 식품위생법, 야생생물법, 약사법, 총포화약법, 축산물위생관리법, 특정범죄가중법 등	관세청 해양경찰청
	밀수출	농수산물품질관리법	
	마약류 범죄	마약류관리법	
	해양산업기술 유출	산업기술보호법, 부정경쟁방지법 등	해양경찰청
	지적재산 침해	상표법 등	
	불법위폐, 외국환거래	외국환거래법, 특정경제범죄법 등	

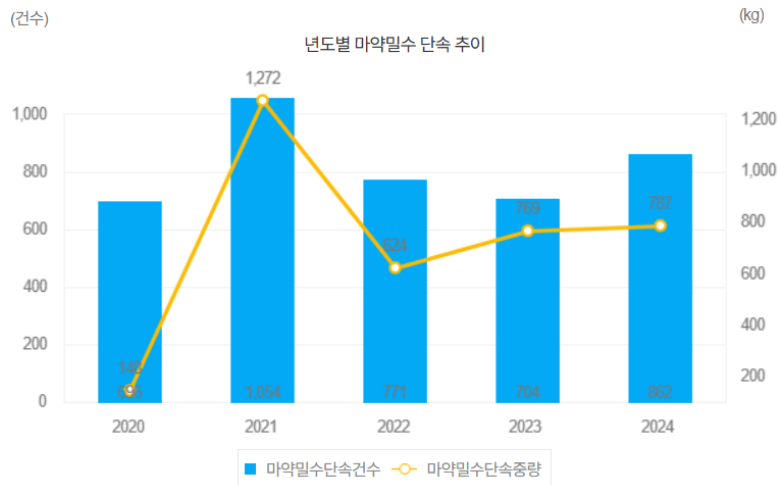
자료: 한국해양수산개발원(2025.5.12.); 해양경찰청(2025) 참조하여 저자 작성

사실 밀입(출)국과 밀수(출)입과 관련된 해양 국제범죄는 매년 지속적으로 발생하는 위협으로 장기적인 효과적 대응을 위해서는 관련 기관 간 협력체계와 범죄 유형의 변화에 따른 적합한 대응체계 개선이 필요하다. 예를 들어, 마약범죄의 경우, 관세청을 포함해 해양경찰청 및 한국마약퇴치운

228) 해양경찰청 보도자료(2024.5.3.)(검색일: 2025.9.9.); 밀항단속법 제1조 참조

동본부(식품의약품안전처)의 마약사범 통계가 최근 급격히 증가했다.[229] 이에, 해양경찰청과 관세청은 증가하는 해상 마약 밀수를 효과적으로 차단하기 위해 2023년 '해상·항만 마약류 범죄 예방 및 단속에 관한 업무협약(MOU)'을 체결하고 기관 간 △ 해양 마약류 범죄 정보교류 활성화, △ 양 기관이 운영 중인 감시프로그램 정보의 신속한 공유, △ 마약탐지견 및 마약류 탐지 장비 등 각 기관의 가용 자원 상호 지원, △ 수사기법 교육 등 역량 강화 분야 지원 등 네 개 분야에 대한 협력을 강화하기로 했다.[230]

〈그림 4-2〉 관세청 연도별 마약사범 단속 현황(2020년~2024년)



자료: 통계청(검색일: 2025.9.9.)

뿐만 아니라, 정부는 마약범죄에 대한 범정부적 대응을 강화하기 위해 2023년 4월 대검찰청, 경찰청, 관세청, 해양경찰청, 국방부, 국가정보원, 식품의약품안전처 등 일곱 개 기관이 참여하는 '마약범죄 특별수사본부'를 설치하고, 온라인 마약거래, 청소년 마약사범, 마약 관련 2차 범죄 등 새로

229) 본 연구보고서 pp. 3-4 참조
230) 해양경찰청 보도자료(2023.4.5.)(검색일: 2025.9.9.)

운 유형의 마약범죄에 효과적으로 대응할 수 있는 체계를 강화하고 있다.[231] 특히, 마약범죄 특별수사본부 설치 이래, 세관과 항만 단계에서의 마약류 단속 및 적발 사례가 증가하는 반면, 단속을 통한 마약 유통 차단은 국내 마약 유통 및 투약 감소로 이어지고 있어 범정부 차원의 마약범죄 대응체계의 긍정적인 효과가 있는 것으로 확인된다.[232] 반면, 해상을 통해 마약 원료가 대량으로 외국에서 국내로 유입되는 사례가 계속 발견되고 있어 이에 대한 단속 방법 고도화, 외국 기관과의 정보협력 등이 지속적으로 이루어져야 할 것으로 생각된다. 특히, 최근 외국인 마약 제조기술자가 국내로 입국하여 국내에서 마약을 제조 및 유통하는 사례가 최근 발견되고 있어 마약 원료 밀수 등과 관련된 조직 범죄 차단과 정보의 협력이 마약 단속의 주요한 방향이 될 것으로 여겨지고 있다.[233]

반면, 이러한 마약범죄 대응체계와 달리, 일반적인 밀수(출)입과 밀입(출)국의 경우, 과거부터 지속적으로 발생하고 있어 현행 대응체계가 효과적으로 운영되고 있는지 의문이다. 해양경찰청 등 유관기관은 매년 해상 밀항·밀입국을 집중 단속하며, 일정한 시기마다 밀수(출)입에 관한 집중 단속 내지 해양 국제범죄 집중 단속을 실시하지만,[234] 실제 밀입(출)국과 밀수(출)입 발생 횟수는 감소하지 않고 있다.

〈표 4-3〉 밀입(출)국 및 밀수(출)입 관련 해양 국제범죄 발생 현황

구분	2020년	2021년	2022년	2023년	2024년
밀입(출)국	69	62	74	74	76
밀수(출)입	70	32	27	53	55

자료: 한국해양수산개발원(2025.5.12.); 해양경찰청(2025) 참조하여 저자 작성

231) 해양경찰청 보도자료(2025.2.17.)(검색일: 2025.9.9.)
232) 위의 자료
233) 위의 자료
234) 경기일보(2024.11.11.)(검색일: 2025.9.9.); 해양경찰청 보도자료(2021.7.19.)(검색일: 2025.9.9.); 해사신문(2024.7.25.)(검색일: 2025.9.9.); DiscoveryNews(2025.5.2.)(검색일: 2025.9.9.)

이는 현재 이러한 범죄에 대응하기 위한 대응체계가 각 기관에 마련되어 있지만, 현행 대응체계가 실제로 위협 억제에 효과적인지 확인을 필요로 하며, 이러한 확인을 통해 장기적인 정책적 개선 방안을 마련해야 할 것을 요구한다. 특히, 과거 밀항은 생계·취업을 목적으로 일본이나 중국 등으로 도항을 시도하는 것이 주된 목적이었으나, 최근에는 주요 경제사범의 처벌 회피, 재산 은닉이 주된 목적으로 사회·경제적 효과가 점점 확대되고 있다. 또한 대규모 밀항자금이 동원되어 중고 수출 선박을 이용하는 등 밀항의 수법 또한 고도화·지능화·은밀화되고 있다. 밀입국 또한 과거 단순히 공해상에서 어선 또는 일반 화물선으로 환승·은닉하여 들어오는 수법이었으나, 최근 밀입국 전문조직과 연계한 고출력 모터보트 내지 소형 고속보트를 이용한 직접 밀입국 시도가 많아지고 있어 점차 범죄 대응이 어려워지고 있다.[235] 밀수(출)입 또한 과거와 달리 점차 지능화·조직화되고 있으며, 마약범죄 수사 집중화로 인한 풍선 효과 등을 고려한 정책적 대응 방안이 마련되어야 한다. 특히, 해양 국제범죄는 권역별로 그 특성이 다르기 때문에 권역별 특성에 따른 적절한 대응 방안이 수립되어야 한다.[236] 이를 위해서는 각 해역 및 연안의 특성과 개별 위협의 위험성 평가 등 객관적 분석을 통해 위협의 변화와 해역의 특성, 취약점을 고려한 적절한 정책적 대응 방안이 수립되어야 한다.

(2) 납치 및 인신매매, 해적 및 무장강도, 불법조업 등

밀입(출)국과 밀수(출)입 외에도 해양 국제범죄에는 납치 및 인신매매, 해

235) 해양경찰청 보도자료(2024.5.3.)(검색일: 2025.9.9.) 등 참조

236) 대한민국 정책브리핑(202.7.25.)(검색일: 2025.9.9.)을 통해 해양경찰청은 해역별 특성을 세 개 권역으로 구분하여 제시하고 있다. 먼저, △ 서해권역은 중국과 가까운 지리적 특성으로 소형보트를 이용한 직접 밀입국 가능성이 높아 리아스식 해안의 특성을 이용 밀항 루트로 이용되며, △ 남해권역도 리아스식 해안의 특성 때문에 국내 경제사범들이 국외 도피 목적으로 밀항 시도와 무사증 입국자의 무단이탈 상륙지로 주로 이용된다고 분석한다. △ 동해권역은 자주 발생하지 않지만 러시아 요트 무단 상륙과 탈북자의 상륙이 우려되는 권역이며, △ 제주권역은 무사증으로 입국하는 외국인들이 육지로 이탈하는 지역적 특성을 가진다고 분석하고 있다.

적 및 무장강도, 불법조업, 해양오염, 기타 범죄가 포함된다. 범죄 유형별로 주요 대응 기관을 살펴보면, 해상에서 발생하는 납치 및 인신매매, 상해·특수상해·폭행·특수폭행·폭행치상 등과 관련된 인권침해와 관련된 해양 국제범죄는 해양경찰청 등 수사기관이 「형법」, 「선박위해처벌법」, 「폭력행위 등 처벌에 관한 법률」(약칭: 폭력행위처벌법) 등에 근거하여 수사 및 단속을 실시한다. 특히, 「선박위해처벌법」은 운항 중인 선박 및 해상구조물에 대한 위해행위를 방지하기 위해 제정되었으며, 관련 규정에 따라 우리나라 관할권 밖에서 운항 중인 우리 국적선 또는 해상구조물의 안전을 위험하게 할 목적으로 선상 또는 해상구조물에 있는 사람을 폭행, 협박, 상해, 살인하는 외국인에게도 적용한다.[237]

외국인권익침해와 관련된 범죄는 「외국인고용법」, 「직업안정법」 등 노동관계 법령을 위반한 경우, 해양경찰청이 해양수산산업 현장에서 불법체류 외국인 고용, 외국인 노동자 인권침해, 임금 체불 등에 대해 출입국·외국인청과 협력하여 단속 및 대응한다.[238] 특히, 법무부 출입국·외국인청은 외국인권익침해와 관련된 해양 국제범죄 단속의 주요 기관으로 필요에 따라 경찰청, 고용노동부, 국토교통부, 해양경찰청 등과 협력하여 합동단속을 실시하기도 한다.[239]

해적의 경우, 주로 우리나라 국적선 및 선원이 승선하고 있는 선박을 해적의 위협으로부터 보호하기 위해 해양수산부와 해군이 협력하여 대응한다. 해적은 유엔해양법협약상 공해 또는 국가 관할권에 속하지 아니한 곳에서 민간 선박이나 항공기 내의 사람이나 재산에 대해 사적 목적으로 범해지는 불법적 폭력행위, 억류 또는 약탈행위로서 사실상 우리나라 관할권 밖에서 이루어지는 해양 국제범죄이다.[240] 이에, 해양수산부는 우리나라

237) 선박위해처벌법 제1조, 제3조 등
238) 해양경찰청 보도자료(2025.3.18.)(검색일: 2025.9.11.)
239) 법무부((2024.12.19.)(검색일: 2025.9.11.); 대한민국 정책브리핑(2025.7.14.)(검색일: 2025.9.11.)
240) 유엔해양법협약 제101조

국적선의 국외 지역에서 해적피해로부터 보호하기 위해 「국제항해선박 등에 대한 해적행위 피해예방에 관한 법률」(약칭: 해적피해예방법)을 제정하고 해적행위와 관련한 정보 수집 및 상황 전파, 해적행위 피해예방 종합대책 수립 및 시행, 해적행위 피해예방을 위한 국제협력 지원, 해적행위 피해예방 종합상황실 운영, 해적행위 피해예방요령 수립 및 시행, 해적행위피해예방협의회 운영 등을 실시하고 있다.[241] 특히, 해군은 해적피해가 높은 북·서인도양 아덴만 해역에 청해부대를 파견하고 있으며, 해양수산부·외교부·해군은 2025년 3월 파견에 앞서 합동해상훈련을 실시하기도 했다.[242]

〈그림 4-3〉 해역별 해적위험지수 현황



자료: 해양안전종합정보시스템(GICOMS)(검색일: 2025.9.11.)

다음으로 우리나라 관할 해역에서 발생하는 외국어선의 불법조업에 대해서는 주로 해양경찰과 해양수산부 어업관리단이 주로 대응하고 있으며, 필요한 경우 해군과 외교부도 협동으로 대응한다. 관련 법령은 「배타적 경제

241) 해적피해예방법 제7조, 제8조, 제6조, 제11조 등 참조

242) 해양수산부 보도자료(2025.3.7.)(검색일: 2025.9.11.) 이 합동해상훈련에서 해양수산부는 해적사건 접수 후 청해부대, 외교부 등 관계기관에 상황을 전파하고, 외교부는 현지 공관과 협력하여 연안국 지원 가능 여부를 파악하고, 해군(청해부대)은 헬기와 고속단정을 투입해 우리 선박과 선원을 구출하고 해적을 진압하는 작전을 실시

수역에서의 외국인어업 등에 대한 주권적 권리의 행사에 관한 법률」(약칭: 「경제수역어업주권법」), 「영해 및 접속수역법」, 「대한민국 정부와 중화인민공화국 정부간의 어업에 관한 협정」, 「불법조업 외국어선 사법처리 절차 등에 관한 규칙」 등이 있다. 해양경찰청과 해양수산부는 관련 법령에 따라 우리나라 배타적 경제수역에서 허가를 받지 않고 조업을 하거나 특정금지구역 등 어업활동 금지 구역에서 어업을 하거나 어업관련 제한 규정을 지키지 않거나, 기타 어업과 관련하여 위법한 어업활동을 한 자와 어선에 대해 단속한다. 단속은 정선 명령을 통해 관련 어업활동을 조사하거나, 위법한 행위가 발견된 경우, 나포하여 벌금을 부과하거나, 어획물을 몰수 또는 압수하거나 어업 허가를 취소하는 등의 조치로 이루어진다.[243]

〈표 4-4〉 해양 국제범죄 유형별 대응 기관

유형	범죄 종류	근거 법령	대응 기관
납치 및 인신매매	납치 및 인신매매	형법, 선박위해처벌법	해양경찰청
해적 및 무장강도	인권침해	형법, 폭력행위처벌법	
	외국인권익침해	외국인고용법, 직업안정법	해양경찰청 고용노동부
	해적	해적피해예방법	해양수산부 외교부 해양경찰청 해군
불법조업	불법조업	영해 및 접속수역법, 경제수역어업주권법 등	
해양오염 등 기타	외국선박 환경오염	항만대기질법, 해양환경관리법	해양경찰청 해양수산부
	기타	검역법, 선박법, 선박안전법 등	

자료: 한국해양수산개발원(2025.5.12.) 참조하여 저자 작성

마지막으로 외국선박 환경오염 범죄 등을 포함한 기타 범죄는 해양경찰청 및 해양수산부가 관련 법령에 따라 대응 및 단속하며, 주요 범죄는 해양오염물질 배출, 선박이나 해양시설로부터 폐기물, 기름, 유해화학물질 등의

243) 경제수역어업주권법 제4조, 제6조, 제6조의2, 제10조-제13조 등; 불법조업 외국어선 사법처리 절차 등에 관한 규칙 제5조 및 제6조, 제10조 등 참조.

무단 방류, 서류 위조, 취업 사기 등 다양한 유형이 존재한다.

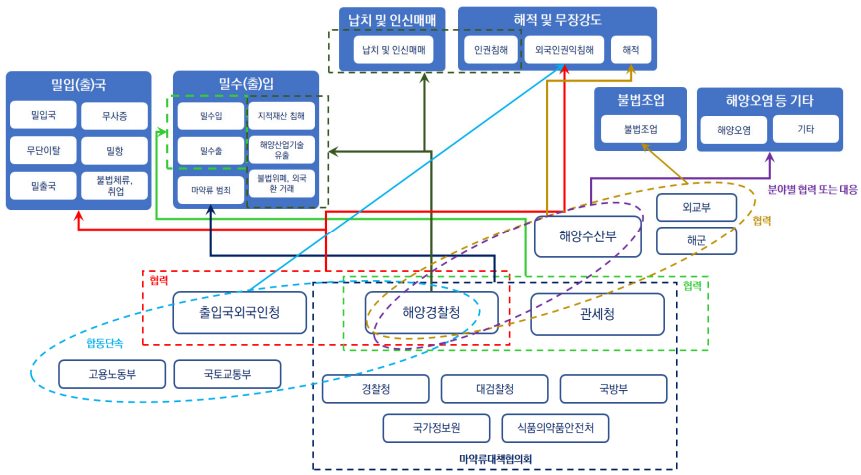
해양 국제범죄는 대상에 따라 직접적으로는 출입국·외국인청을 포함하여 관세청, 해양경찰청, 해양수산부가 대응하고 있으며, 간접적으로는 외교부, 고용노동부, 국가정보원, 국방부, 해군 등 다양한 기관이 대응체계를 구성한다.[244] 다만, 이러한 다양한 기관이 해양 국제범죄에 대응함에도 불구하고, 마약 등 사회적으로 영향이 막대한 범죄를 제외하고 범부처 협의체 등 일원화된 대응체계를 확인하기는 어렵다. 앞 장에서 살펴본 바와 같이 최근 해양 국제범죄는 단독범죄보다 조직화, 광역화, 전문화되고 있으며 이에 범행 진행에 따라 여러 부처가 관련될 여지가 다분히 존재한다. 이에 따라 해양 국제범죄를 효과적으로 단속하기 위해서는 다양한 기관들의 협력 내지 공조 체계가 제도적으로 확보되어야 하며, 협력체계의 범위 또한 확대해 나가야 한다. 반면, 현재의 해양 국제범죄에 대한 대응체계는 〈그림 4-4〉에서 확인할 수 있는 바와 같이 특정 기관의 요청에 따라 타방 기관이 협력에 응하는 수동적인 협력체계가 주를 이루고, 제도상 유기적인 협력체계 또는 일원화된 협력체계를 기대하기는 어렵다.

이는 범행의 과정이 다수의 관할 범위 또는 대상을 걸쳐 나타나는 해양 국제범죄에 기관의 특성 및 역할에 따라 분절적으로 대응하게 되어 실질적인 범죄 억제 효과를 기대하기 어렵게 한다. 이에 최근 변화하고 있는 해양 복합위협의 한 유형인 해양 국제범죄에 효과적으로 대응하기 위해서는 국내 유관기관 간의 일원화된 유기적 협력체계가 제도적으로 구축되어야 하며, 또한 이러한 제도를 장기적으로 확대해 나가야 할 것으로 판단된다.[245]

244) 한국해양수산개발원(2025.5.12.); 관세법; 출입국관리법, 폭력행위처벌법, 해적피해예방법, 경제수역어업주권법, 해양환경관리법, 검역법, 선박안전법 관련 법령 등 참조.

245) 박주상·박동균, 앞의 책, pp. 77-79. 해양 국제범죄의 국내외 기관 간 협력체계 내지 공조체계 미흡과 관련된 보다 상세한 내용은 본 논문을 참조

〈그림 4-4〉 해양 국제범죄 대응체계



자료: 저자 작성

2) 해양 국제범죄 관할별 대응체계

해양 국제범죄의 관할별 대응체계는 크게 「국제선박항만보안법」에 따른 항만시설과 「해양경비법」에 따른 경비수역, 그 외 「관세법」, 「출입국관리법」 등 개별법에 따른 국경 관리 지역으로 구분할 수 있다.

「국제선박항만보안법」은 "국제항해에 이용되는 선박과 그 선박이 이용하는 항만시설의 보안에 관한 사항을 정하고 국제항해와 관련한 보안상의 위협을 효과적으로 방지하여 국민의 생명과 재산을 보호"하기 위해 제정되었다.[246] 「국제선박항만보안법」은 국제항해에 이용되는 선박과 그 선박이 이용하는 항만시설을 국제항해선박과 선박항만연계활동이 가능하도록 갖추어진 시설로 정의하고, 이러한 항만시설에서 발생하는 보안사건을 국제항해선박소유자와 항만시설소유자가 1차적으로 대응 및 관리하도록 정하

246) 국제선박항만보안법 제1조

고 있다.[247] 여기서 보안사건은 "국제항해선박이나 항만시설을 손괴하는 행위 또는 국제항해선박이나 항만시설에 위법하게 폭발물 또는 무기류 등을 반입·은닉하는 행위 등 국제항해선박·항만시설·선박항만연계활동 또는 선박상호활동의 보안을 위협하는 행위 또는 그 행위와 관련된 상황"을 의미하며, 해양 복합위협의 해양 국제범죄, 해양테러 등을 포함하는 개념이라고 할 수 있다.[248]

이러한 위협에 대응하기 위해 「국제선박항만보안법」은 항만시설에서 국제항해선박소유자와 항만시설소유자가 보안사건에 대응하기 위해 취해야 하는 조치를 정하고 있는데 먼저, 국제항해선박소유자는 보안 책임자를 지정하고, 자신이 소유하거나 관리·운영하는 선박에 대한 보안평가를 실시하고, 선박보안계획서를 작성하여 해양수산부 장관에게 승인을 요청하여야 한다. 또한 국제항해선박소유자는 정기적 또는 필요에 따라 선박보안심사를 해양수산부로부터 받아야 하며, 선박보안과 관련된 증서 및 서류를 선박에 비치하도록 조치하여야 한다.[249]

다음으로 항만시설소유자 또한 보안 책임자를 지정하고, 항만시설보안평가를 실시하여야 하며, 항만시설보안계획서를 작성하여 해양수산부로부터 승인을 받아야 한다. 또한, 항만시설소유자 또한 해양수산부로부터 항만보안심사를 받고 관련 증서와 서류를 당해 항만에 비치하여야 한다. 국제항해선박소유자와 달리 항만시설소유자는 국제항해여객선 승객 등에 대한 보안검색 또한 실시해야 한다. 다만 이 경우, 보안검색 중 신체 및 휴대물품의 보안검색은 관할 경찰관서의 장이 지도·감독하고, 위탁수하물의 보안검

247) 국제선박항만보안법 제7조, 제23조. 이들 규정은 국제항해선박소유자와 항만시설소유자가 자신이 소유하거나 관리·운영하는 국제항해선박항만시설의 보안업무를 효율적으로 수행하게 하기 위하여 자격을 갖춘 보안 책임자를 지정하여 선박보안평가, 선박보안계획서의 작성 및 승인신청, 내부보안심사, 항만시설보안계획서의 작성 및 승인신청, 항만시설의 보안점검, 항만시설 보안장비의 유지 및 관리 등을 수행하도록 정하고 있다.

248) 국제선박항만보안법 제2조, 제5호

249) 국제선박항만보안법 제7조-제11조

색에 대해서는 관할 세관장이 지도·감독하도록 「국제선박항만보안법」은 정하고 있다. 항만시설소유자는 보안을 확보 및 유지하고 보안검색을 실시하기 위해 관련 경비·검색인력을 확보하고 보안시설·장비 또한 확보해야 한다. 또한 항만시설의 범죄 예방 및 보안을 확보하기 위해 폐쇄회로 텔레비전 또한 설치해야 한다.[250]

「국제선박항만보안법」은 국제항해선박소유자와 항만시설소유자에게 보안사건 예방 및 대응하도록 정하고 있지만, 실제 이들의 대응조치 범위는 관련 계획 수립과 심사 수검, 보안평가 실시 등으로 제한되며, 항만시설소유자의 경우, 보안인력 및 시설 확보 및 유지 등을 포함한 업무로 제한된다. 사실상 항만시설에서 보안사건 내지 사고가 발생했을 때, 이를 경찰청 등 단속기관에 신속하게 전파하고 관련 기관이 조사·단속을 실시할 수 있도록 상황을 관리하는 것이 국제항해선박소유자와 항만시설소유자의 권한 범위라고 할 수 있다.

공간적으로 「국제선박항만보안법」이 적용되는 곳은 국제항해선박과 선박항만연계활동이 가능한 항만시설은 「국제선박항만보안법」에 따라 「선박안전법」 제2조 제1호에 따른 선박으로 국제항해에 이용되는 선박의 기항이 가능한 곳으로 「항만법」 제2조에 따른 전국 31개 무역항이다. 이와 더불어, 「국제선박항만보안법 시행규칙」은 선박을 수리하거나 건조하는 조선소의 선박계류시설, 석유 비축기지, 액화천연가스 생산기지 또는 화력발전소의 선박계류시설, 해양수산부 장관의 허가를 받아 외국 국적 선박이 기항하는 불개항장의 선박계류시설 또한 「국제선박항만보안법」이 적용되는 항만시설로 규정하고 있다.[251]

250) 국제선박항만보안법 제23조-제26조, 제30조의2, 제31조, 제31조의2
251) 항만법 제2조 제5호; 국제선박항만보안법 제2조; 국제선박항만보안법 제2조 등

〈표 4-5〉 항만법 제2조 제5호의 항만시설

구분	항만시설
국가관리무역항(14개)	경인항, 인천항, 평택·당진항, 대산항, 장항항, 군산항, 목포항, 여수항, 광양항, 마산항, 부산항, 울산항, 포항항, 동해·묵호항
지방관리무역항(17개)	서울항, 태안항, 보령항, 완도항, 하동항, 삼천포항, 통영항, 장승포항, 옥포항, 고현항, 진해항, 호산항, 삼척항, 옥계항, 속초항, 제주항, 서귀포항

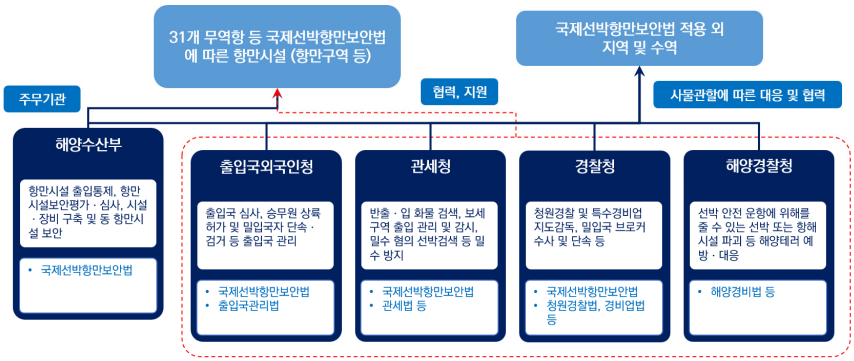
자료: 항만법 제2조 제5호

사실상 국제항해선박이 정박 또는 계류할 수 있는 모든 시설이 「국제선박항만보안법」에 적용을 받게 되며, 이들 항만시설에 대해서는 1차적으로 해양수산부가 관할권을 가지고 국제항해선박소유자와 항만시설소유자가 보안사고를 관리하고 초동 조치를 취하고 상황을 전파한다. 다만, 「국제선박항만보안법」에 따라 제정된 「항만 출입절차에 관한 규정」에 의해 화재, 재난·재해, 인명사고 및 범죄 발생 등 긴급한 상황 발생 시, 경찰관, 해양경찰관 및 소방관은 보안검색 절차를 생략하고 항만시설에 출입할 수 있고, 관련 범죄를 수사 및 단속할 수 있다. 그리고 「국제선박항만보안법」이 적용되지 않는 지역의 경우 앞에서 살펴본 바와 같이 유형별 대응체계에 따라 수상구역은 주로 해양수산부와 「해양경비법」에 따른 해양경찰이, 연안 등 해양과 연계된 육상구역의 경우 「출입국관리법」에 따른 출입국·외국인청과 「관세법」에 따른 관세청 등 기타 유관기관과 해양경찰이 위협에 대응한다.

다만, 앞서 살펴본 해양 국제범죄 유형별 대응체계를 고려할 때, 기관 간 단속 및 대응 과정에서 「국제선박항만보안법」에 따른 공간적 관할권이 다소 불명확한 측면이 존재한다. 이 법은 항만시설 소유자의 보안업무 구역을 항만시설로 규정하고 있으며 항만시설은 기본시설인 수역시설·외곽시설·임항교통시설·계류시설과, 기능시설인 보조시설·하역시설·여객이용시설·화물 유통 및 판매시설·선박보급시설·항만시설용 부지 및 지원시설·항만친수시설·항만배후단지 등을 포함한다. 즉, 항계 내 육상과 수상시설 전반을 포괄한다고 볼 수 있다. 따라서 해양수산부 등 「국제선박항만보안법」

에 따른 보안사고 대응 기관은 항만의 육상 및 수상구역에서 발생하는 보안사고를 예방하고 초동 조치를 취해야 한다.

〈그림 4-5〉「국제선박항만보안법」에 따른 대응체계



자료: 함혜현·전봉조·이장욱(2022), p. 380; 국제선박항만보안법을 참조하여 저자 작성

그러나 제2장에서 살펴본 사례에서 확인할 수 있듯, 항만공사와 항만보안공사 등 항만시설소유자는 주로 육상 항만시설에서 발생하는 밀입국 시도 등 보안사고에 중점을 두고 예방활동을 수행하고 있다. 또한 관련 보안시설 규정 역시 대부분 육상 항만구역 감시를 위한 장비와 시설에 집중되어 있다.[252] 이에 따라 항만구역 내 수상구역에서 보안사고가 발생하거나, 육상에서 수상구역으로 연계되는 사건이 발생할 경우, 항만시설 소유자는 「해양경비법」에 따라 수상구역에서 일반사법경찰권을 가진 해양경찰에 협조를 요청하게 된다. 이러한 구조는 하나의 연속된 사건에 대해 기관 간 단절적 대응을 유도하고, 자체적 감시·자원을 활용한 능동적 대응보다는 요청에 의존한 수동적 대응으로 흐르기 쉽다. 이는 고속보트 등을 활용한 조직적 밀입(출)국이 빈번해지고 있는 최근의 해양 복합위협 상황을 고려할

252) 함혜현·전봉조·이장욱(2022), pp. 391-392; 국제선박항만보안법 제31조, 제31조의2; 국제선박항만보안법 시행규칙 제40조 등 참조

때 그 심각성이 더욱 커진다고 할 수 있다.[253]

2. 해양테러 국내 대응체계

해양테러는 앞에서 정의한 바와 같이 전통 해양테러, 해저시설 공격, 대량살상무기 위협, 드론 등 무인체계 위협 등으로 구분할 수 있다.

〈표 4-6〉 해양테러 유형 및 행위

구분	유형	주요 행위
해양테러	• 해양테러	• 연안 주요시설(발전소, 주요 항만 등) 위협, 연안 다중이용시설(여객선, 여객터미널 등) 공격 등
	• 해저시설 공격	• 해저케이블, 가스 수송관 등 공격
	• 대량살상무기 위협	• 대량살상무기 위협, 대형 환경오염 피해 등
	• 드론 등 무인체계 위협	• 드론, 무인 해상정 등을 활용한 연안 주요시설 위협 등

자료: 저자 작성

이러한 해양테러는 주로 「테러방지법」에 규율을 받는다. 「테러방지법」 제2조는 테러를 "국가·지방자치단체 또는 외국 정부의 권한행사를 방해하거나 의무 없는 일을 하게 할 목적 또는 공중을 협박할 목적으로 하는 행위"로 정의한다.[254] 그리고 해양과 관련된 테러 행위는 같은 법에서 "선박 또는 해상구조물과 관련된 행위"로서 운항 중인 선박 또는 해상구조물을 파괴하거나, 그 안전을 위태롭게 할 만한 정도의 손상을 가하는 행위, 폭행이나 협박, 그 박의 방법으로 운항 중인 선박 또는 해상구조물을 강탈하거나 선박의 운항을 강제하는 행위, 운항 중인 선박의 안전을 위태롭게 하기 위하여 그 선박 운항과 관련된 기기·시설을 파괴하거나 중대한 손상을 가하거나 기능장애 상태를 일으키는 행위로 구분하고 있다.[255] 선박과 해상

253) 보다 상세한 사항은 위의 논문, pp. 390-391 참조.
254) 테러방지법 제2조 제1호

구조물에 대한 구체적인 테러 행위 외에도 테러방지법은 테러를 일으킬 목적으로 사람을 살해하거나 사람의 신체를 상해하여 생명에 대한 위험을 발생하게 하는 행위 또는 사람을 체포·감금·약취·유인하거나 인질로 삼는 행위, 사망·중상해 또는 중대한 물적 손상을 유발하도록 제작되거나 그러한 위력을 가진 생화학·폭발성·소이성 무기나 장치를 차량 또는 시설에 배치하거나 폭발시키거나 그 밖의 방법으로 사용하는 행위, 핵물질, 방사성물질 또는 원자력시설을 파괴하여 생명·신체 또는 재산을 해하거나 공공의 안전을 위태롭게 하는 행위, 이러한 시설을 부당하게 조작하여 생명이나 신체에 위험을 가하는 행위 등 또한 구체적 테러 행위로 규정하고 있다.[256] 이에 해양 복합위협으로서 해양테러로 분류하고 있는 해양테러, 해저시설 공격, 대량살상무기 위협, 드론 등 무인체계 위협 등도 광의의 범위에서 「테러방지법」상 테러 행위에 포섭될 수 있을 것으로 판단된다.

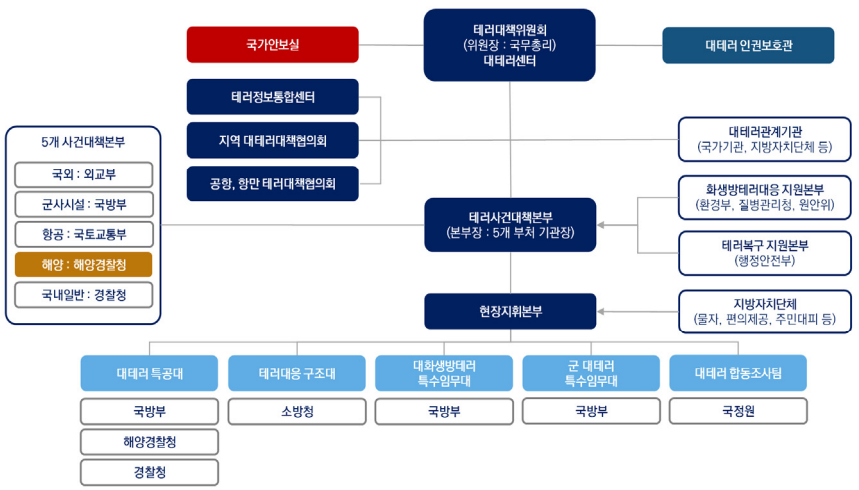
「테러방지법」은 이러한 테러 행위에 대응하기 위해 국가 테러대책기구로서 국가테러대책위원회를 설립하고 관련 정책을 수립하고 평가하며 관련 기관의 역할을 분담·조정·심의·의결하도록 정하고 있다. 특히, 해양경찰청은 「테러방지법 시행령」 제14조에 따라 해양테러가 발생하거나 발생할 우려가 현저한 경우에 국가테러대책위원회 테러사건대책본부를 설치·운영하는 기관으로 해양테러 대응을 주관하는 기관이다. 더불어 해양경찰청은 「테러방지법 시행령」 제12조, 제13조에 따라 지역 테러대책협의회와 공항·항만 테러대책협의회를 구성하여 지역, 항만, 공항 등에서 해양과 관련된 테러가 발생했을 때, 협의회를 통해 대테러 업무를 수행한다.

「테러방지법」 제10조는 테러 예방을 위해 관계기관의 장이 국가중요시설과 다수가 이용하는 시설 및 장비에 대한 테러예방대책과 테러의 수단으로 이용될 수 있는 폭발물·총기류·화생방물질, 국가 중요행사에 대한 안전

255) 테러방지법 제2조 제1호 다목
256) 테러방지법 제2조 제1호 가목, 라-마목

관리대책을 수립하도록 정하고 있다. 해양경찰청은 「테러방지법」상 이러한 안전관리대책을 수립하기 위해 「해양경비법」 제16조의2에 따른 해양 대테러 계획을 5년마다 수립한다. 특히, 해양 대테러 계획에는 국내외 테러 정세 및 전망 분석, 해양 대테러 조직·인력·시설·장비의 확충·관리, 해양 대테러 역량 강화, 해양테러 관련 정보의 수집·교환, 국내외 대테러 유관기관과의 유기적 협력체제 구축 등이 포함되어 있어, 최신 해양테러 유형 등을 반영한 해양 대테러 활동이 가능하도록 한다.[257]

〈그림 4-6〉 「테러방지법」상 테러 대응체계



자료: 테러방지법; 대테러센터(검색일: 2025.9.13.) 참조하여 저자 작성

다만, 「테러방지법」은 해양테러의 정의와 범위를 별도의 규정으로 정하고 있지 않아 앞에서 설명한 바와 같이 선박 등 해양에서 시작하여 파괴 등 테러 행위가 종국적으로 육상 주요시설에서 구성될 때, 이를 어떤 기관이 주관하여 담당는지 책임성이 분명하지 않을 수 있다. 그럼에도 불구하고 테러와 관련된 활동은 테러대책위원회와 대테러센터를 중심으로 관계기

257) 해양경비법 시행규칙 제2조의2.

관의 대테러활동 역할의 분담과 조정이 테러 정세에 따라 유기적으로 이루어지고 있는 것으로 보인다. 특히, 「테러방지법」을 통해 대테러 활동을 테러 관련 정보의 수집, 테러위험인물의 관리, 테러에 이용될 수 있는 위험물질 등 테러수단의 안전관리, 인원·시설·장비의 보호, 국제행사의 안전확보, 테러위협에의 대응 및 무력진압 등 테러 예방과 대응에 관한 제반 활동 등 대테러 활동에 필요한 사항을 구체적으로 정하고 있어 해양경찰청은 해양과 연계된 테러 정세를 파악하여 관련된 활동을 실시한다.[258]

〈표 4-7〉 대테러활동 개념

예방·대비	대응(사건 발생)	수습·복구
• 테러정보 수집·전파 • 신고체계 확립 • 테러대상시설 및 테러이용 수단 선별·관리 • 대테러 인력·시설·장비·물자 확보 • 긴급대응체계 구축 • 테러대응 교육·훈련	• 비상연락 • 비상대피 • 상황보고 • 긴급 대응체계 가동 – 사건대책본부 및 현장지휘본부 가동(해양테러 – 해양경찰청) • 긴급 구조·구호	• 물리적 수습·복구 – 피해시설 응급 복구 – 시설·시스템 정상화 • 심리적 수습 복구 – 피해가족 지원 – 국민 심리 안정 – 사상자 치료 및 장례지원 • 피해확산 방지

자료: 국무조정실 대테러센터(2023), p. 3.

3. 해양 사이버위협 국내 대응체계

국내 해양 사이버위협에 대응하는 체계는 크게 해양수산부를 중심으로 수립되고 있는 해사 사이버안전 관리 체계와, 해양경찰청을 중심으로 이루어지고 있는 사이버범죄의 대응체계이다.

해양수산부는 2023년 자율운항선박 개발 등 육상과 선박 간 정보통신망·시스템의 연결성이 확대됨에 따라 해사 사이버 공격·위협에 선제적으

258) 테러방지법 제2조 제6호

로 대응하고, 산업계의 해사 사이버안전 관리 체계 구축지원에 관한 제도적 기반을 마련하기 위해 「해사 사이버안전 관리지침」을 제정했다.[259] 이 지침을 통해 해양수산부는 해사 사이버 공격·위협을 "해킹, 컴퓨터 바이러스, 서비스 거부, 전자기파 등 전자적 수단으로 선박 운항 시스템 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·훔치는 행위 및 그와 관련된 위협"으로 정의한다.[260] 그리고 이러한 사이버 공격·위협에 대응하기 위해 해양수산부 장관은 △ 관련 대책을 수립하여 시행할 수 있으며, △ 전문기술인력 확보 및 양성, 교육프로그램 개발 등을 위한 필요한 조치, △ 전략·기술을 연구·개발하고 선박 및 사업장 등에 대한 보급 등을 실시할 수 있다.[261] 또한, 해양수산부 장관은 해사 사이버안전 확보를 위해 필요한 경우 선박 및 사업장에 대한 진단 또는 실태평가를 실시할 수 있다.[262]

「해사 사이버안전 관리지침」은 선박소유자가 효과적인 해사 사이버안전 관리를 위해 고려해야 하는 자산관리, 업무분장 및 위험성 평가 등을 규정하고 있으며, 더불어 선박소유자가 해사 사이버안전 관리 체계를 구축하는 경우 고려해야 하는 보호조치, 탐지조치, 대응조치, 복구조치 등 또한 규정하고 있다.[263]

마지막으로 「해사 사이버안전 관리지침」은 해사 사이버 공격·위협으로 인한 선박 운항불가 등 해양사고가 발생하거나 발생할 우려가 있는 경우에 선박소유자가 피해를 최소화하는 조치를 실시하고, 해양수산부 장관에게 통보하도록 정하고 있으며, 해양수산부는 이와 같은 통보를 받은 경우 관련 부서·기관 등에 전파·보고하고, 사고 대응 및 복구지원 조치 등을 할

259) 해양수산부 보도자료(2023.4.21.)(검색일: 2025.9.13.)
260) 해사 사이버안전 관리지침 제2조
261) 해사 사이버안전 관리지침 제4조
262) 해사 사이버안전 관리지침 제5조
263) 해사 사이버안전 관리지침 제10조-제16조

수 있도록 정하고 있다.[264]

〈그림 4-7〉「해사 사이버안전 관리지침」상 해사 사이버안전 보안 체계



자료: 해사 사이버안전 관리지침을 참조하여 저자 작성

「해사 사이버안전 관리지침」은 현재 해양수산부고시로 제정되어 있으며 사이버안전 대책 수립, 진단 또는 실태평가 등 주요 정책적 수단이 권고사항으로 정해져 있어 해양 사이버위협에 대한 실질적인 효과를 가지기는 어려운 것으로 보인다. 또한, 현재 이 지침의 적용 범위는 선박 및 사업장을 대상으로 하고 있어 항만 등에서 발생하는 사이버침해 사고에는 적용하기 어려울 수 있다. 뿐만 아니라 지침은 해양 사이버 공격 및 위협 자체보다 이들로 인한 해양사고가 발생하거나 발생할 우려가 있는 경우 이를 해양수산부 장관에게 관련 사항을 통보하도록 정하고 있다. 따라서 사이버 공격 및 위협이 사업장의 선박운항관리시스템 등에만 발생하고 선박의 운항 안전에 직접적인 영향이 없을 때, 이러한 사이버 공격 및 위협을 해양수산부에 통보해야 하는지 모호하다. 또한 사이버 공격 및 위협이 발생했을

264) 해사 사이버안전 관리지침 제17조

때, 이러한 사고가 해양사고의 위험성과 연계되는 것을 평가하여 해양수산부에 통보해야 하는데, 이에 대한 객관적 평가기준을 지침은 제공하고 있지는 않다.[265] 다만, 해양 사이버위협에 대응하기 위한 기능적 고려사항, 단계별 조치 사항 등을 포함하고 있어, 사이버위협 대응보다 예방을 위한 실무 지침을 제공한다고 할 수 있다.

해양경찰청 또한 해양 사이버위협에 대응하기 위해 2023년 2월 사이버수사 전담 조직을 신설하고 정보통신망 침해, 정보통신망의 불법적 이용, 불법 콘텐츠 유포 및 공유 등에 대한 범죄를 본격적으로 대응하기 시작했다.[266]

〈표 4-8〉 해양 사이버범죄 유형

유형	예시
정보통신망 침해	• 항만시설 등 해킹, 침입, 자료 유출, 변조 등
정보통신망 이용	• 인터넷을 통한 밀수·밀입국·무사증 범죄 및 불법거래 등
불법콘텐츠 범죄	• 불법 선원구직 사이트, 불법 낚시어선의 낚시객 모집 등

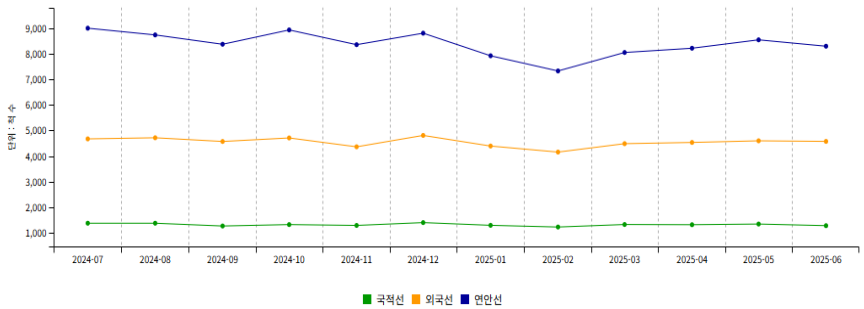
자료: 해양경찰청 보도자료(2023.12.29.)(검색일: 2025.9.13.)

현재 해양경찰청은 해양 사이버범죄에 대응하기 위해 본청 수사국 내 과학수사팀에 사이버수사계를 설치하여 운영하고 있으며, 더불어 남해지방해양경찰청 수사과에도 사이버수사계를 설치하여 운영하고 있다. 해양경찰 본청 사이버수사계의 경우, 과학수사팀 예하에 소속되어 있어 디지털 포렌식 감식업무, 중요사건 과학수사업무지원을 포함하여 해양 사이버범죄에 관한 정책을 주로 담당하며, 따라서 사이버수사 기획, 지휘·감독·지원, 전문인력 양성·교육, 수사기법·프로그램·장비 연구 개발 등을 담당한다.[267]

265) 해양수산부 보도자료(2024.10.31.)(검색일: 2025.9.7.) 해양수산부는 이러한 우려에 대응하기 위해 2024년 해사 사이버안전 관리 강화방안을 수립하고 향후 민·관 합동 사이버사고 대응 훈련을 실시하고, 선박소유자 등이 사이버안전 관리 체계를 구축할 수 있는 사고 대응·복구에 관한 표준지침서를 제공하며, 해사 사이버안전에 관한 인증제도를 도입한다고 발표했다.
266) 해양경찰청 보도자료(2023.12.29.)(검색일: 2025.9.13.)
267) 해양경찰청 사무분장규칙 제24조; 해양경찰청(검색일: 2025.9.13.)

남해지방해양경찰청 사이버수사계는 실질적인 사건 대응을 중심으로, 사이버범죄수사, 관련 수사 기획·지도, 수사관련 교류 및 협력 등을 주로 수행한다.[268] 해양경찰청은 대외무역의존도가 높은 우리나라의 경제 특성과 한해 우리나라에 입항하는 선박의 수가 약 30,000척에 이르는 것을 고려하고, 최근 선박의 항해·통신·안전관리 등 전 분야에 위성통신·위치확인시스템(GPS) 등 첨단 정보화 기술이 활용되고 있어 해양 사이버위협이 증가하고 있다고 판단하고, 사이버 수사 교육을 강화하고, 전문 경력자를 채용하는 한편, 다크웹 및 가상화폐 추적시스템을 도입하여 해양에 특화된 수사기법을 확보할 예정이다.[269]

〈그림 4-8〉 선박입항 통계(2024~2025)



자료: 국가물류통합정보센터(검색일: 2025.9.13.)

사실 우리나라는 국가 및 공공기관에 대한 사이버위협에 대해서 국가안보실과 국가정보원을 중심으로 국가 사이버위협 대응체계를 이미 구축하고 있다. 그리고 일반 시민 및 기업 등 민간을 대상으로 발생하는 사이버위협의 경우 과학기술정보통신부와 경찰청을 중심으로 사이버위협에 대응하고 있다. 특히, 국가정보원은 국가사이버안보센터를 예하에 설치하여 국가 사이버위기관리 주관기관으로서 역할하고 있다. 국가사이버안보센터는 「사

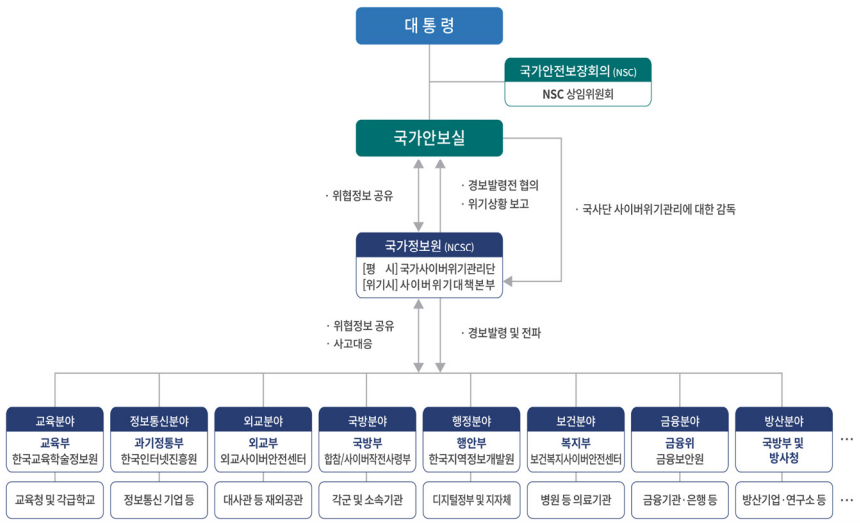
268) 남해지방해양경찰청과 그 소속기관 사무분장 규칙 제11조
269) 해양경찰청 보도자료(2023.12.29.)(검색일: 2025.9.13.)

이버안보 업무규정」에 따라 정부 차원에서 사이버 공격·위협을 즉시 탐지·대응하기 위해 통합보안관제체계를 구축하여 운영하고 있다.

통합보안관제체계는 다른 중앙행정기관의 보안관제센터와 연계하여 사이버 공격 및 위협을 탐지·대응하는 보안관제를 실시한다. 국가·공공기관에 대한 보안관제는 국가보안관제(국가사이버안보센터), 부문보안관제(중앙행정기관), 단위보안관제(각급기관)의 3단계 체계로 이루어지며, 국가사이버안보센터는 국가보안관제센터로서 부문 및 단위 보안관제센터의 효과적 사이버 공격·위협 탐지 및 차단을 위해 관련 기술을 배포하고 국가적 차원에서 안보를 위협하는 사이버 공격을 탐지 및 대응한다. 국가사이버안보센터는 사이버 공격·위협의 주요 유형을 이메일 무단열람, 해킹메일 유포, 경유지 구축, 악성코드 유포 등으로 분류하고, 보안관제를 통해 실시간으로 이러한 사이버 공격·위협을 탐지하여, 피해를 최소화하며, 관계기관과 신속한 정보 공유를 통해 유기적인 대응이 가능하도록 한다. 특히 보안관제센터별(국가, 부문, 단위 등) 수집된 사이버 공격·위협 정보가 다를 경우, 탐지·분석한 공격정보를 실시간으로 공유하여 국가 차원의 사이버위협에 종합적·체계적 대응이 가능하도록 유도한다.[270] 부문별로 과학기술정보통신부와 한국인터넷진흥원(KISA)은 민간 분야 침해사고 예방, 정보 공유, 교육 및 컨설팅 등 실무 대응에 주력한다. 국방부는 군 전산망과 핵심기술에 대한 방어, 사이버작전사령부를 중심으로 군사적 위협에 대응하며, 실제 해킹 경유지나 악성코드 발견 시 정보 공유를 통해 피해의 확산을 방지한다.

270) 국가사이버안보센터, 사이버위협 대응(검색일: 2025.9.13.)

〈그림 4-9〉 국가사이버안보 수행체계



자료: 국가사이버안보센터, 국가사이버안보 수행체계(검색일: 2025.9.13.)

경찰청 또한 사이버범죄수사과, 사이버테러대응과를 두어 사이버사기 사건 수사 및 단속을 실시하고 피싱, 파밍, 스미싱 등 사이버금융범죄, 사이버도박 사건, 그 외 정보통신망을 이용한 사이버범죄에 대응한다. 또한 경찰청 사이버테러대응과는 사이버 공간에서의 침해·안보 위협 사건을 수사하고 계정 도용, 정보통신망 침입 등 해킹 사건, 서비스거부(DDoS) 사건, 악성프로그램 관련 사건, 사이버 개인정보·위치정보침해범죄 사건 등 또한 수사하고 대응한다.[271]

271) 경찰청과 그 소속기관 직제 제19조; 경찰청과 그 소속기관 직제 시행규칙 제16조

제2절 해양 복합위협 발생 현황 및 GIS 분석

본 절에서는 해양 복합위협의 경향을 분석하기 위해 해양 국제범죄의 발생 현황을 분석한다. 앞에서도 언급한 바와 같이 해양 복합위협은 크게 해양 국제범죄, 해양테러, 사이버위협이 혼합하여 복합적으로 나타나는 위협을 해양 복합위협으로 정의할 수 있다. 그러나 해양 국제범죄를 제외하고 해양테러, 해양 사이버위협으로 분류되어 관리되는 통계는 없다. 이에, 해양경찰청 등 관련 기관에서 보유하고 있는 해양 국제범죄 통계를 분석하여 간접적으로 해양 복합위협에 관한 경향성을 분석한다.

또한 본 절에서는 해양 국제범죄의 발생 위치와 관련 기관의 관서 위치의 상관관계를 분석한다. 이를 통해 해양 국제범죄에 대응하는 국가 자원과 범죄 발생과의 상관관계를 도출하고 이를 통해 효과적인 범죄 대응을 위한 국가기관 간의 협력체계에 대한 함의를 도출하고자 한다.

1. 해양 복합위협 발생 현황 분석

1) 해양 국제범죄 유형별 경향 분석

(1) 연도별 해양 국제범죄 발생 현황 분석

2020년부터 2024년까지 국제범죄 발생 건수는 총 1,248건, 연평균 발생 건수는 약 250건으로 '20년 이후 감소세를 나타낸 이후 '22년부터 다시 증가하였다. '20년에는 311건으로 최근 5년간 가장 많은 범죄가 발생하였으며, 특히 출입국관리법 위반이 46건, 마약류관리법 위반이 37건으로 전체 범죄의 약 27%를 차지하였다.[272] '21년에는 220건으로 지난해 대비 감소폭이 가장 컸으며, 특히 식품위생법 위반 19건 감소, 마약류관리법 위

반 16건 감소, 검역법 위반 열 건 감소 국민사회안전 분야에서 가장 큰 감소폭을 보였다.[273] '22년에는 총 205건으로 가장 적은 범죄 발생 건수를 보이며, 특히 환경보존 분야 중 항만대기질법, 해양환경관리법 위반에서 총 22건으로 큰 감소폭을 보였다.[274] '23년에는 총 250건으로 지난해 대비 국민사회안전 분야 및 인권보호 분야 범죄 발생 건수가 증가하였으며, 특히 외국인고용법 위반 사례가 지난해 두 건 대비 20건으로 급증하였다.[275] '24년에는 총 262건으로 지난해 대비 12건 증가하였으며 특히 밀수입·수출 분야에서 야생생물법 위반 사례가 지난해 0건 대비 22건으로 급증하였다.[276] 종합하면 '21~'22년 사이에는 발생 건수가 감소하였는데, 코로나 팬데믹으로 인한 국제 이동 제한, 교역 감소 등이 주요 원인으로 해석된다. '23년 이후 다시 증가세로 전환되어 전반적인 회복세가 나타났으며, 특히 밀수입·수출, 인권 관련 범죄는 경제 활동 재개와 직접적으로 연관이 있을 것으로 판단할 수 있다.

〈표 4-9〉 연도별 국제범죄 발생 건수 현황

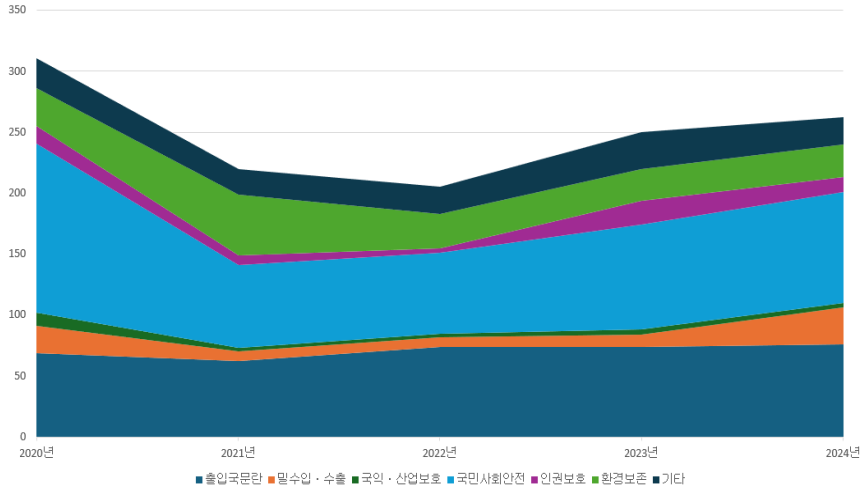
단위: 건

범죄 유형	'20년	'21년	'22년	'23년	'24년	합계
출입국문란	69	62	74	74	76	355
밀수입·수출	22	8	8	10	30	78
국익·산업보호	11	3	3	4	4	25
국민사회안전	139	68	66	86	91	450
인권보호	14	8	4	20	12	58
환경보존	31	50	28	26	27	162
기타	25	21	22	30	22	120
총계	**311**	**220**	**205**	**250**	**262**	**1248**

자료: 해양경찰청(2025) 참조하여 저자 작성

272) 해양경찰청(2025)
273) 해양경찰청(2025)
274) 해양경찰청(2025)
275) 해양경찰청(2025)
276) 해양경찰청(2025)

〈그림 4-10〉 국제범죄 발생 건수(2020년~2024년)



자료: 해양경찰청(2025) 참조하여 저자 작성

(2) 해양 국제범죄 유형별 발생 현황 분석

해양 국제범죄를 '출입국문란, 밀수입·수출, 국익·산업보호, 국민사회안전, 인권보호, 환경보존, 기타' 등 일곱 개 유형으로 구분하여 연도에 따른 증감 경향을 파악하였다.

'출입국문란'은 2020년 69건에서 2024년 76건으로 소폭 증가하였는데, 전체적으로는 일정 수준을 유지하고 있으나, 다소 점진적 상승세를 보였다. '밀수입·수출'은 2021년~2022년은 정체(여덟 건)였으나, 2024년에 급격히 증가(30건)하였는데, 세계 경제 회복 및 국제 무역량 증가에 따라 불법 밀수입·수출 활동이 다시 활성화된 것으로 보인다. '국익·산업보호'는 2020년 11건에서 2024년 네 건으로 전체적으로 낮은 건수를 유지하였는데, 국제 통상 환경 안정화 및 산업 보호 제도 강화의 영향을 받은 것으로 추정된다. '국민사회안전'은 2020년 139건에서 '21년 68건으로 약 51%

감소한 후 다시 증가하여 2024년에는 91건을 기록하였다. 사회안전 이슈가 급격히 줄어든 후 점진적으로 회복하는 패턴을 보였다. '인권보호'는 2022년에 최저(네 건)를 기록한 후, 2023년에 20건으로 급증하였는데, 난민, 분쟁 등 글로벌 이슈가 반영된 것으로 추정된다. '환경보존'은 2021년에 급증(50건)하였으나 이후 다시 감소하고 있다. 국제 환경규제 강화 및 이행 상황에 따라 영향을 받은 것으로 해석된다. '기타'는 2020년 25건에서 2024년 22건 수준으로 비교적 안정적이나, 2023년에 일시적 증가(30건)가 있었다.

〈표 4-10〉 범죄 유형별 발생 건수 통계분석(2020년~2024년)

단위: 건

범죄 유형	평균 발생 건수	표준편차	최솟값	최댓값
출입국문란	71.0	5.02	62	76
밀수입·수출	15.6	9.14	8	30
국익·산업보호	5.0	3.49	3	11
국민사회안전	90.0	28.98	66	139
인권보호	11.6	5.46	4	20
환경보존	32.4	9.23	26	50
기타	24.0	3.80	21	30

자료: 해양경찰청(2025) 참조하여 저자 작성

범죄 유형별 발생 건수에 대한 기초통계분석 결과 '국민사회안전'은 평균 발생 건수가 가장 높았으며, 변동성도 큰 편이었다. '국익·산업보호'는 평균 발생 건수와 변동성이 가장 낮아, 상대적으로 안정적인 범죄 유형으로 판단된다. '밀수입·수출', '환경보존' 역시 변동성이 큰 유형으로 나타났다.

2) 해양 국제범죄 시계열 분석

(1) 계절별 해양 국제범죄 경향 분석

2020년부터 2024년까지 국제범죄 발생 건수 총 1,248건 중 봄(3월~5월)에 발생한 범죄 건수는 284건(약 23%), 여름(6월~8월)에 발생한 건수는 229건(약 18%), 가을(9월~11월)에 발생한 건수는 366건(약 29%), 겨울(12월~2월)에 발생한 건수는 369건(약 30%)으로 나타났다. 봄의 경우 국민사회안전 분야의 범죄가 104건으로 약 37%를 차지하며. 출입국문란 범죄가 67건으로 약 24%를 차지하였다. 여름의 경우 출입국문란 범죄가 70건으로 약 31%를 차지하며, 국민사회안전 분야의 범죄가 62건으로 약 27%를 차지하였다. 가을의 경우 국민사회안전 분야의 범죄가 137건으로 약 37%를 차지하며. 출입국문란 범죄가 115건으로 약 31%를 차지하였다. 겨울의 경우 국민사회안전 분야의 범죄가 147건으로 약 40%를 차지하며. 출입국문란 범죄가 103건으로 약 28%를 차지하였다.

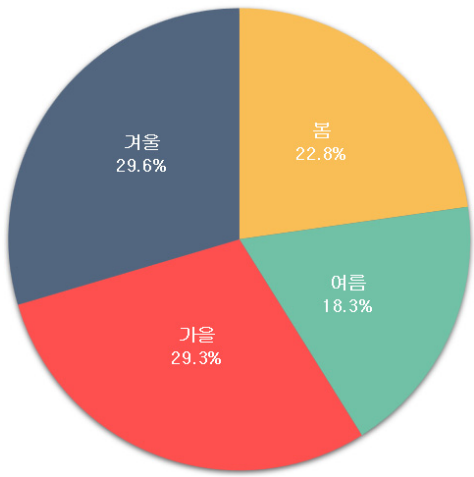
〈표 4-11〉 계절별 발생 건수 분석(2020년~2024년)

단위: 건

범죄 유형	봄	여름	가을	겨울
출입국문란	67	70	115	103
밀수입·수출	21	9	12	36
국익·산업보호	10	6	5	4
국민사회안전	104	62	137	147
인권보호	16	14	12	16
환경보존	42	40	46	34
기타	24	28	39	29

자료: 해양경찰청(2025) 참조하여 저자 작성

〈그림 4-11〉 계절별 해양 국제범죄 발생 현황



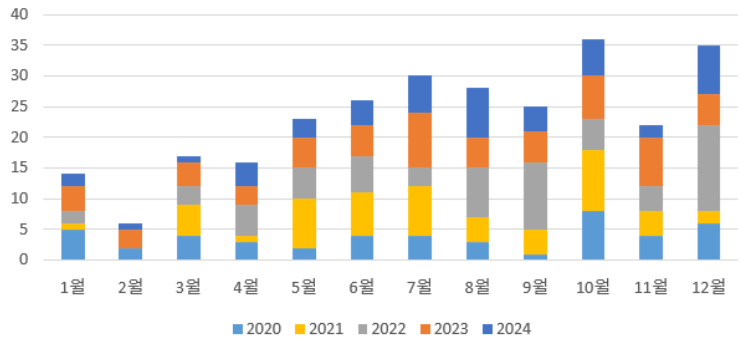
자료: 해양경찰청(2025) 참조하여 저자 작성

(2) 월별 해양 국제범죄 경향 분석

출입국문란 범죄 중 출입국관리법 위반 범죄는 총 278건이며, 10월에 36건으로 가장 많았으며, 2월에 여섯 건으로 가장 적었다.[277] 계절별 고려 시 여름에 84건으로 약 30%를 차지하며, 겨울에 55건으로 약 20%를 차지하였다. 범죄 최대 발생 계절과 최소 발생 계절의 차이는 10%p인 점을 고려할 때, 출입국관리법 위반 범죄의 경우 계절의 영향보다 시기(연초 또는 연말)의 영향이 크다고 볼 수 있다.[278]

277) 해양경찰청(2025)
278) 해양경찰청(2025)

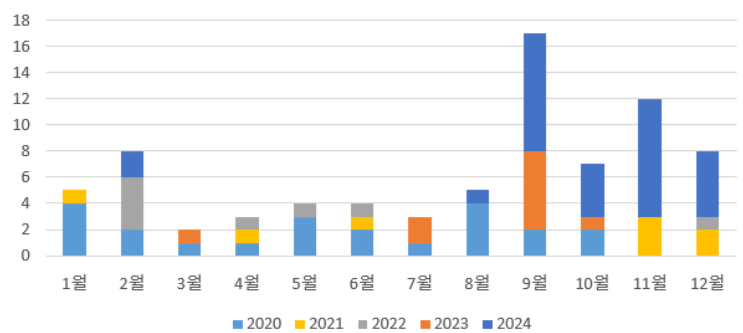
〈그림 4-12〉 월별 출입국문란 범죄 현황



자료: 해양경찰청(2025) 참조하여 저자 작성

밀수입·수출 범죄의 경우 총 78건이며, 9월에 17건으로 가장 많았으며, 3월에 두 건으로 가장 적었다. 계절별 고려 시 가을에 36건으로 약 46%를 차지하며, 봄에 아홉 건으로 약 12%를 차지하였다.[279] 범죄 최대 발생 계절과 최소 발생 계절의 차이가 34%p로 크게 나타나지만, 연도별 범죄 발생 빈도가 고르지 않다는 점에 대한 고려가 필요하다.[280]

〈그림 4-13〉 월별 밀수입·수출 범죄 현황

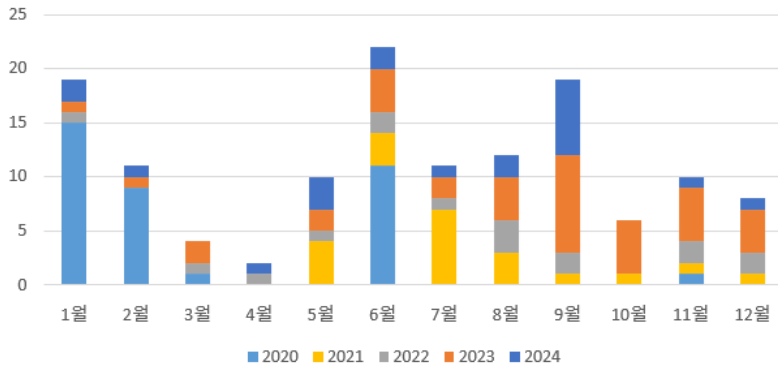


자료: 해양경찰청(2025) 참조하여 저자 작성

279) 해양경찰청(2025)
280) 해양경찰청(2025)

국민사회안전 범죄 중 마약류관리법 위반 범죄는 총 134건이며, 6월에 22건으로 가장 많았으며, 4월에 두 건으로 가장 적었다.[281] 계절별 고려 시 여름에 45건으로 약 34%를 차지하며, 겨울에 16건으로 약 12%를 차지하였다.[282] 최대 발생 계절과 최소 발생 계절의 차이가 약 24%p인 점과 최근 범죄 건수의 변화 양상을 고려했을 때 마약류관리법 위반 범죄의 발생 시기가 여름~가을로 이동하고 있음을 확인할 수 있었다.[283]

〈그림 4-14〉 월별 마약류관리법 범죄 현황



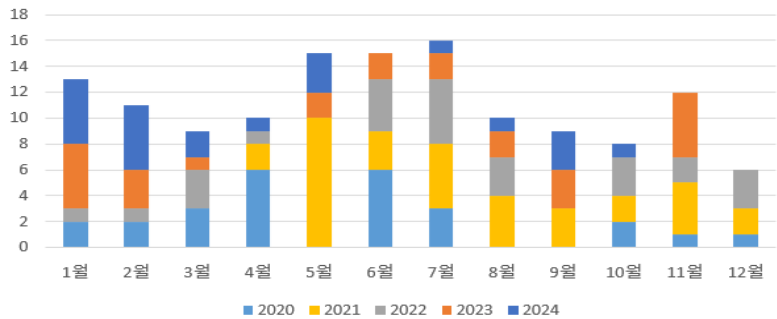
자료: 해양경찰청(2025) 참조하여 저자 작성

환경보존 범죄 중 해양환경관리법 위반 범죄는 총 134건이며, 7월에 16건으로 가장 많았으며, 12월에 여섯 건으로 가장 적었다.[284] 계절별 고려 시 여름에 41건으로 약 31%를 차지하며, 가을에 29건으로 약 22%를 차지하였다.[285] 최대 발생 계절과 최소 발생 계절의 차이가 약 9%p인 점과 월별 범죄 분포를 고려했을 때 봄~여름에 해양환경관리법 위반이 상대적으

281) 해양경찰청(2025)
282) 해양경찰청(2025)
283) 해양경찰청(2025)
284) 해양경찰청(2025)
285) 해양경찰청(2025)

로 자주 발생함을 확인할 수 있었다.[286]

〈그림 4-15〉 월별 해양환경관리법 범죄 현황



자료: 해양경찰청(2025) 참조하여 저자 작성

(3) 시간대별 해양 국제범죄 경향 분석[287]

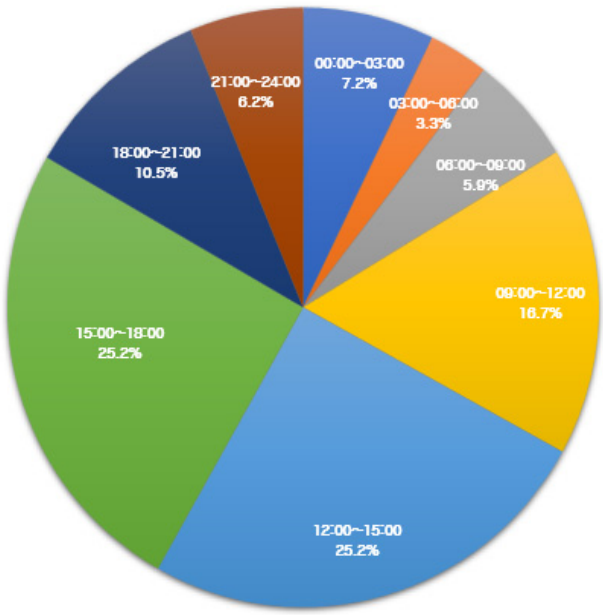
'24년에 발생한 국제범죄 현황 총 306건 중 가장 많은 범죄가 발생한 시간대는 12:00~15:00와 15:00~18:00로 각 77건(약 25%) 발생하여 두 시간대를 합치면 전체의 절반 이상을 차지하였다. 일반적인 근무시간인 09:00~18:00에 발생한 범죄는 전체의 약 67%에 해당하며, 이외의 시간대인 33% 중 18:00~21:00가 약 10%, 00:00~03:00가 약 7%를 차지하였다. 00:00~03:00에 발생한 범죄 총 22건 중 국경침해가 아홉 건으로 약 41%를 차지하였으며, 출입국 위반이 여섯 건으로 약 27%를 차지하였다. 03:00~06:00에 발생한 범죄가 총 열 건으로 전체 시간대 중 가장 적었으며, 국경침해가 네 건으로 약 40%를 출입국 위반이 세 건으로 약 30%를 차지하였다. 이 밖에 먹거리 관련 양식산업발전법 및 원양산업발전법에서 각 한 건씩 위반 사례가 발생하였다. 06:00~09:00에 발생한 범죄 총 18건 중 국경침해가 일곱 건으로 약 39%를 차지하였으며, 출입국 위반 및 환경

286) 해양경찰청(2025)
287) 해양경찰청(2025)의 데이터를 참조하여 저자 작성

오염법이 각 세 건으로 16.7%를 차지하였다. 09:00~12:00에 발생한 범죄 총 51건 중 출입국 위반이 17건으로 약 33%를 차지하였으며, 밀수가 열 건으로 약 20%를 차지하였다. 출입국 위반 범죄(총 63건) 중 약 27%가 해당 시간대에 발생하여 타 시간대 대비 가장 높은 비율을 기록하였다. 12:00~15:00에 발생한 범죄 총 77건 중 밀수가 23건으로 약 30%, 먹거리 범죄가 15건으로 약 20%를 차지하였다. 밀수의 경우 해당 시간대에 전체 발생 건수(총 63건) 대비 약 37%가 발생하여 타 시간대 대비 가장 높은 비율을 기록하였다. 또한 환경오염 범죄의 경우 해당 시간대에 전체 발생 건수(총 27건) 대비 약 33%가 발생하여 타 시간대 대비 가장 높은 비율을 기록하였다. 15:00~18:00에 발생한 범죄 총 77건 중 먹거리 위반이 20건으로 약 26%, 국경침해 및 밀수가 각 19건으로 약 25%를 차지하였다. 먹거리 범죄의 경우 해당 시간대에 전체 발생 건수(총 46건) 대비 약 43%가 발생하여 타 시간대 대비 가장 높은 비율을 기록하였다. 국경침해 또한 해당 시간대에 전체 발생 건수(총 70건) 대비 약 27%가 발생하여 타 시간대 대비 높은 비율을 기록하였다. 18:00~21:00에 발생한 범죄 총 32건 중 출입국 위반이 아홉 건으로 약 28%를 차지하였으며, 국경침해가 일곱 건으로 약 22%를 차지하였다. 21:00~24:00에 발생한 범죄 총 19건 중 마약류 관리법 위반이 여섯 건으로 약 32%를 차지하였으며, 국경침해가 다섯 건으로 약 26%를 차지하였다. 마약류법 위반의 경우 해당 시간대에 전체 발생 건수(총 21건) 대비 약 29%가 발생하여 타 시간대 대비 가장 높은 비율을 기록하였다.[288]

288) 해양경찰청(2025)

〈그림 4-16〉 시간대별 범죄 발생 현황

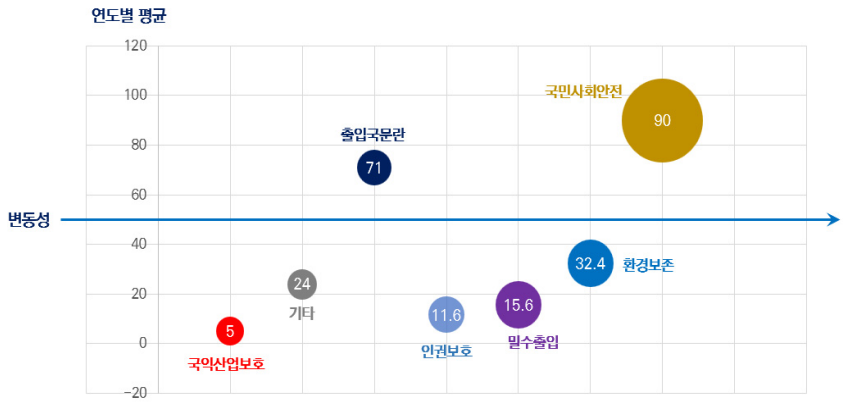


자료: 해양경찰청(2025) 참조하여 저자 작성

3) 해양 국제범죄 발생 현황 분석 시사점

해양 국제범죄는 코로나 팬데믹 시기인 2020년부터 2022년까지 다소 감소했으나, '22년 이후 지속적으로 증가추세에 있는 것으로 분석되었다. 이를 연도별 변동성과 발생 평균을 기준으로 분석하면 〈그림 4-17〉과 같이 분석할 수 있다. 먼저, 연도별로 발생 건수가 높으면서 변동성이 높은 것은 국민사회안전과 관련된 범죄로 나타났으며, 이들 범죄는 변동성에 대한 관리와 동시에 범죄 증감에 대응하는 것 또한 필요하다.

〈그림 4-17〉 연도별 평균 발생 현황과 변동성



주: 원의 크기가 클수록 연도별 변동성이 높은 해양 국제범죄
자료: 해양경찰청(2025) 참조하여 저자 작성

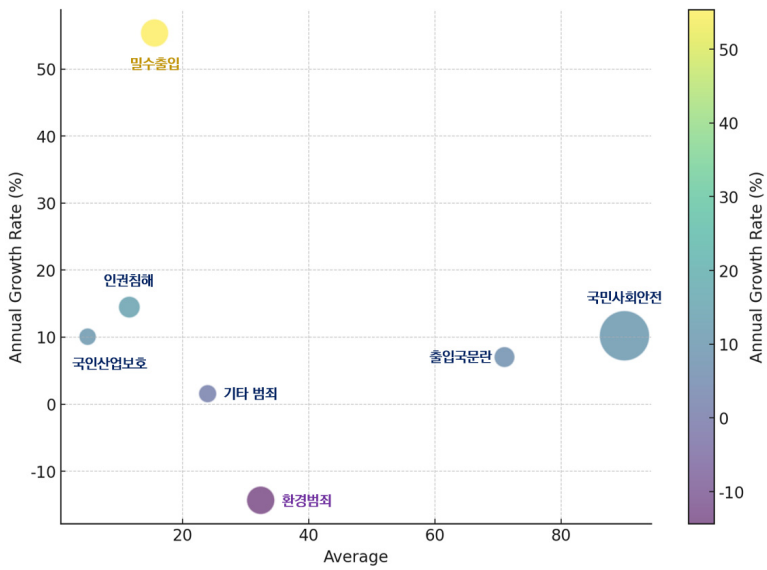
이를 위해서는 단기적으로 범죄 발생을 억제 및 관리하기 위한 범죄의 원인을 분석하여 현재의 자원을 효과적으로 활용할 수 있는 방안을 마련해야 한다. 또한 장기적으로는 범죄의 변동성을 관리 및 대응하기 위해 범죄의 경향, 동향, 원인 등을 다층적으로 분석하여 조직, 자원 등을 적절히 배분하는 장기적 정책적 대응 방안이 필요할 것으로 판단된다. 연도별 범죄 발생의 변동성이 높다는 것은 범죄의 양상이 원인과 사회적 환경에 따라 지속적으로 변화하여 다각적인 정책 대안이 필요하다는 것을 의미한다. 뿐만 아니라, 범죄의 높은 변동성은 당해 범죄의 암수율이 높다는 것을 의미할 수도 있기 때문에, 범죄의 양성화를 위한 사회적 대응을 비롯하여, 범죄 관리, 통계분석 등 다양한 범죄 분석 기법과 정책적 대응 방안이 동원되어야 한다.[289]

환경보존, 밀수(출)입 등과 관련된 해양 국제범죄는 장기적인 정책 방안을 중심으로 동향 및 경향, 사회적 요인 등을 분석하여 다가적 대응 방안을

289) 박성수·백민석(2019), pp. 247-248. 마약범죄의 암수율을 근거로 통계만으로 마약범죄 대응방안을 수립하기보다 범죄 관리를 위한 다각적 방안이 수립되어야 할 것을 언급. 보다 상세한 사항은 논문을 참조.

수립해야 하며, 출입국문란 등 밀입(출)국과 관련된 범죄는 범죄 발생 자체를 억제하기 위한 단기적 선진화된 수사기법 및 대응 자원 등을 확보해야 할 것으로 보인다. 다만, 아래 환경범죄는 사실상 연도별 증가율이 마이너스로 매년 환경범죄가 약 10% 이상 감소하고 있는 것으로 나타나고 있어, 현재의 대응체계가 효과적으로 작용하고 있다고 할 수 있다.

〈그림 4-18〉 연도별 발생 현황, 증가율, 변동성 분석 결과



주: 원의 크기가 클수록 연도별 변동성이 높은 해양 국제범죄
자료: 해양경찰청(2025) 참조하여 저자 작성

따라서 위의 표를 근거로 현재 장·단기적으로 우선적으로 대응해야 하는 해양 국제범죄는 국민사회안전과 관련된 범죄와, 밀입(출)국과 관련된 출입국문란, 밀수(출)입 등이다.

2. 해양 복합위협 GIS 분석

1) 분석개요

'21년부터 '24년까지의 국제범죄 발생 건수는 총 1,144건이며, 각 범죄의 위치정보는 범죄 발생 위치를 기준으로 Google Sheet의 Geocode by Awesome Table 부가기능을 활용하여 십진수 형태의 위도/경도 좌표로 변환하였다.[290] 또한 해상에서 발생한 범죄의 경우 육상 행정구역을 반영하기 위해 인근 도서 지역 또는 육지로 전환하였다. 국제범죄와 관련된 관계기관은 해양경찰서(파출소), 관세청, 출입국·외국인청(사무소 및 출장소 포함), 지방고용노동청(지청 및 출장소 포함), 지방식품의약품안전청, 지방해양수산청으로 선정하였다. 국제범죄와 관계기관의 상관관계를 분석하기 위해 범죄의 분야 및 종류별로 관계기관을 배정하였다. 범죄 분야의 경우 '출입국문란', '밀수입·수출', '국익·산업보호', '국민사회안전', '마약류 범죄', '인권보호', '환경보존', '기타'로 구분하였다. 이는 해양경찰청이 해양 국제범죄를 관리하기 위해 분류하고 있는 유형이며, 본 장 제1절에서 분석한 해양 국제범죄의 유형과의 관계는 〈표 4-12〉와 같다.

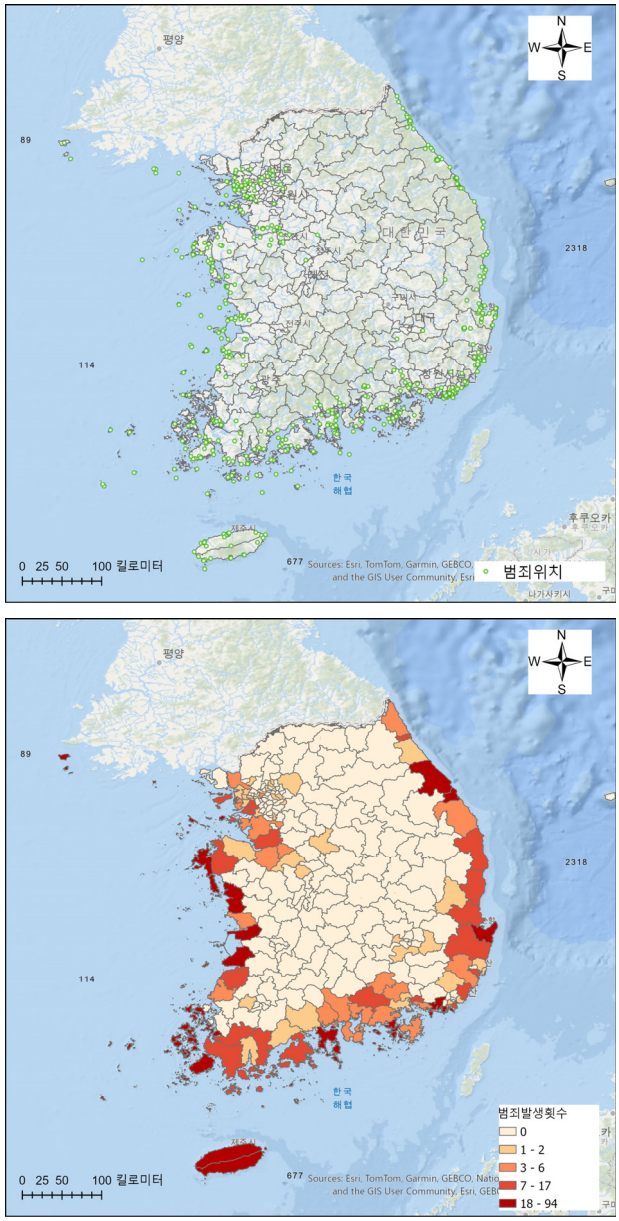
〈표 4-12〉 범죄 분야별 관계기관 배정

해양경찰 국제범죄 유형	관계기관	관련 해양 복합위협 국제범죄 유형
출입국문란	출입국·외국인청	밀입(출)국
밀수입·수출	관세청	밀수(출)입
국익·산업보호	해양경찰청	
국민사회안전	지방해양수산청	
마약류 범죄	지방식품의약품안전청	
인권보호	지방해양수산청	납치
		해적 및 무장강도
환경보존	지방해양수산청	기타
기타	지방해양수산청	불법조업, 기타

자료: 해양경찰청(2025) 참조하여 저자 작성

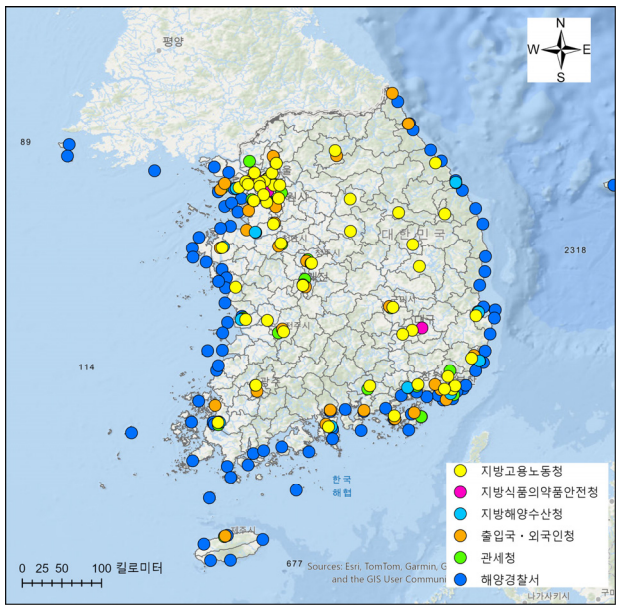
290) Talarian(검색일: 2025.9.13.)

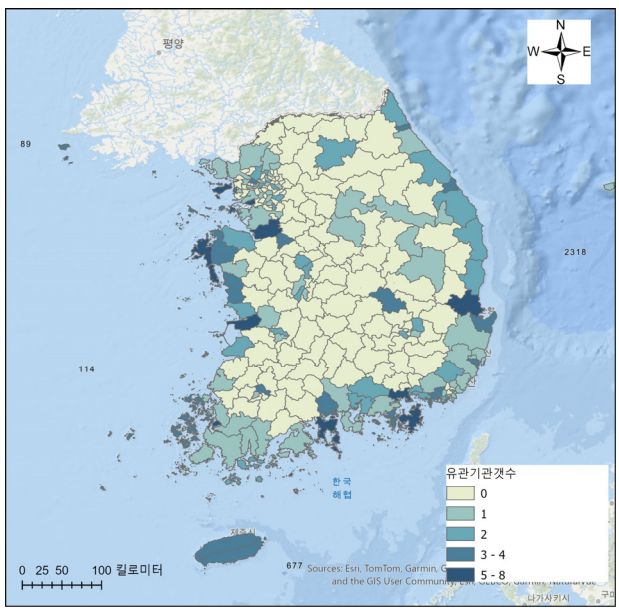
〈그림 4-19〉 범죄 발생 위치, 시군구별 범죄 발생 횟수



자료: 해양경찰청(2025) 참조하여 저자 작성

〈그림 4-20〉 국제범죄 관계기관 위치, 시군구별 기관 개수





자료: 해양경찰청(2025) 참조하여 저자 작성

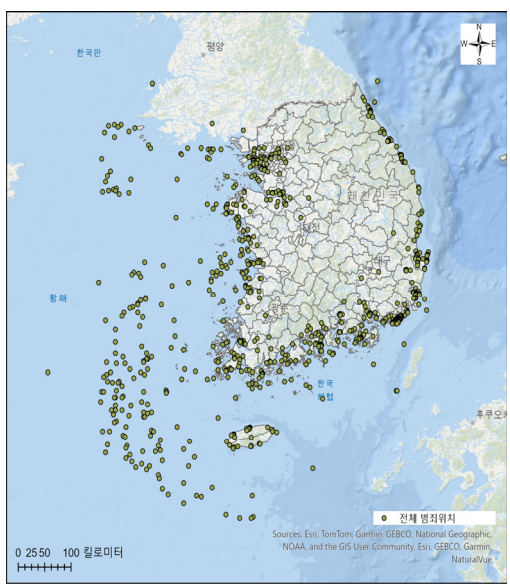
2) 범죄별 핫스팟 분석 결과

(1) 계절별, 시간대별 범죄 핫스팟 분석

우리나라에서 발생하는 국제범죄의 계절별, 시간대별 경향성을 파악하기 위해 핫스팟 분석을 시행하였다. 핫스팟 분석은 데이터에서 통계적으로 유의미한 핫스팟을 식별하기 위해 Getis-Ord Gi* 통계를 활용하며, 공간적 군집의 유의성을 검증해 특정 지역에 사건이 과도하게 집중되는지(Hot Spot)를 판별할 수 있다.

핫스팟 분석에서는 해상에서의 좌표를 명확하게 반영하였다. 해상에서의 국제범죄는 동해안·남해안 대비 서해안에서 주로 발생하였으며, 전체 범죄의 범위는 위도 32.183N ~ 38.633N, 경도 123.1E ~ 129.583E 내에 분포하고 있다.

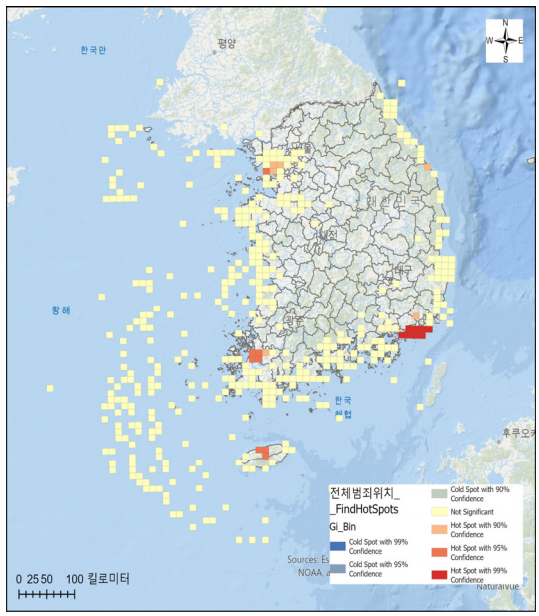
〈그림 4-21〉 해양 국제범죄 분포 위치



자료: 해양경찰청(2025) 참조하여 저자 작성

전체 국제범죄에 대한 핫스팟 분석 결과 부산에서 가장 강한 핫스팟을 보이며, 목포, 제주, 인천 순으로 핫스팟 결과를 나타낸다. 분석 해역의 전체 범위 대비 국제범죄 발생 수는 적기 때문에 콜드스팟은 생성되지 않음을 알 수 있다.

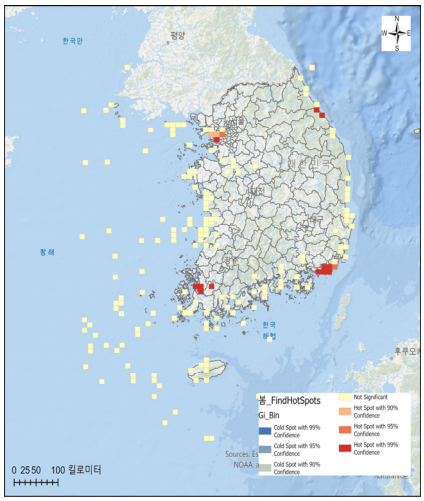
〈그림 4-22〉 해양 국제범죄 핫스팟 분석 결과



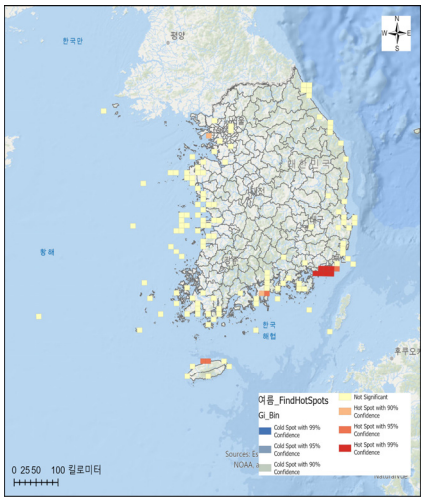
자료: 해양경찰청(2025) 참조하여 저자 작성

계절별 핫스팟 분석 결과 부산 지역은 일괄되게 해양 국제범죄 핫스팟을 보이고 있다. 봄의 경우 목포, 인천 및 일부 강원권에서도 핫스팟을 나타낸다. 여름의 경우 타 계절 대비 연안에서 범죄가 자주 발생하며, 가을의 경우 반대로 대양에서 범죄가 자주 발생하는 양상을 보인다.

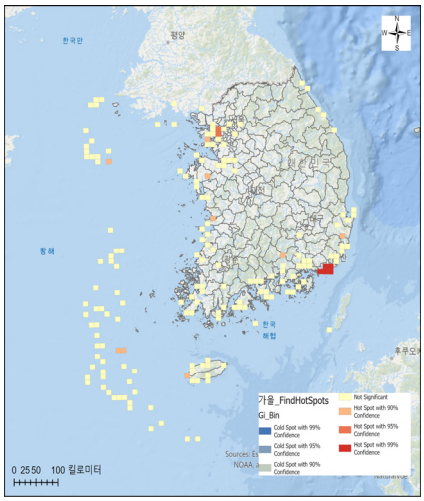
〈그림 4-23〉 해양 국제범죄 계절별 핫스팟 분석 결과



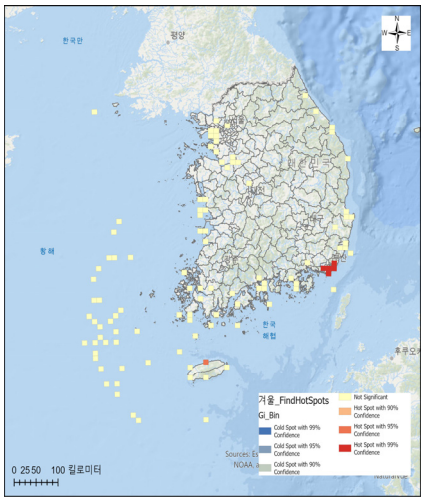
봄



여름



가을

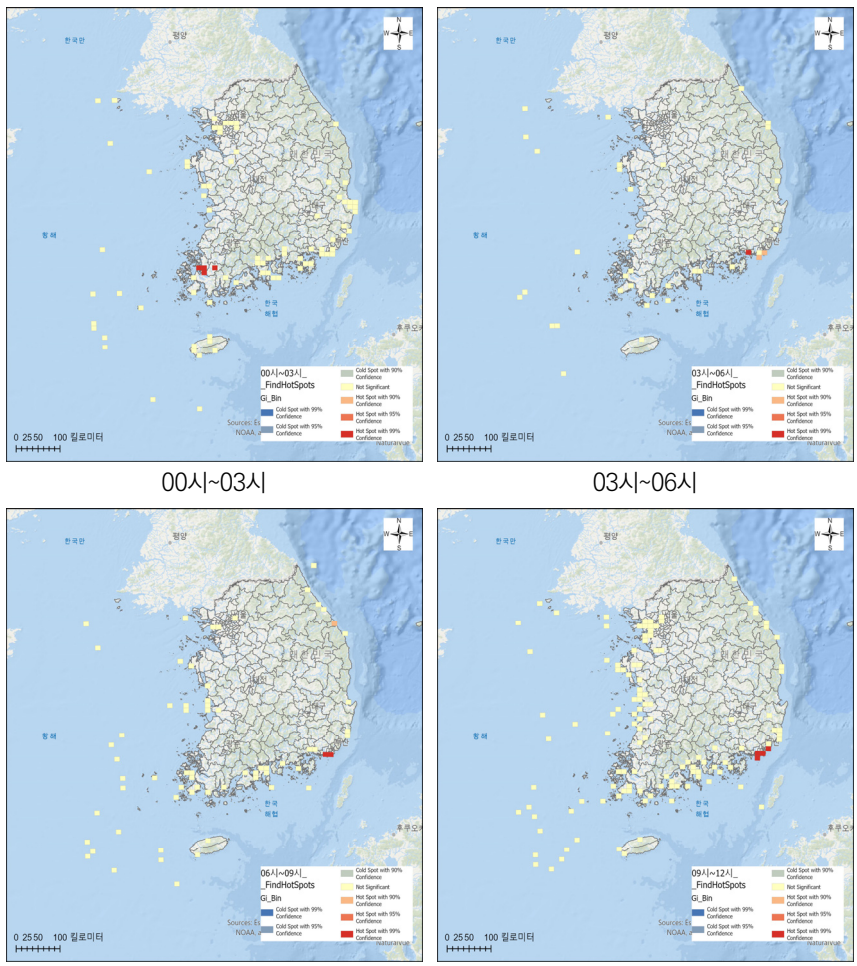


겨울

자료: 해양경찰청(2025) 참조하여 저자 작성

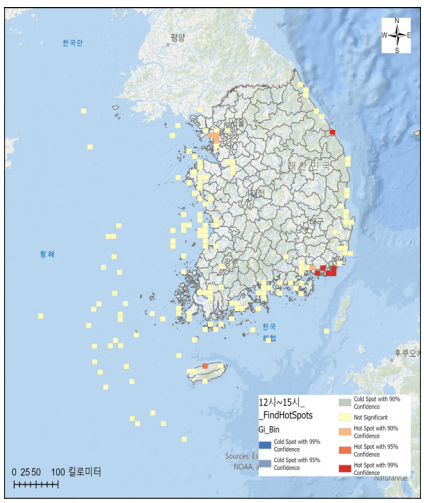
시간대별 핫스팟 분석 결과 부산 지역은 일괄되게 국제범죄 핫스팟을 보이고 있다. 00시~03시의 경우 목포 지역에서, 15시~18시의 경우 군산 지역에서 일시적으로 핫스팟이 나타나지만, 타 지역의 경우 유의미한 차이를 나타내지 않는 것으로 분석된다.

〈그림 4-24〉 시간대별 핫스팟 분석 결과(00시~12시)

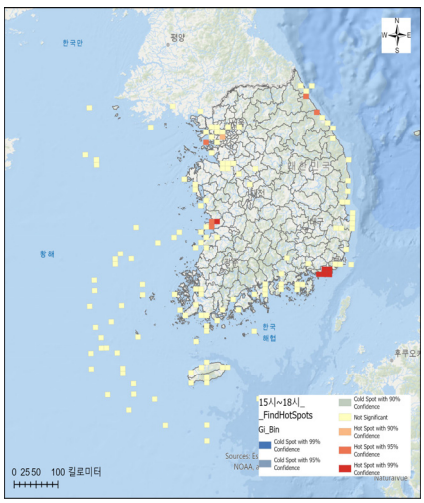


자료: 해양경찰청(2025) 참조하여 저자 작성

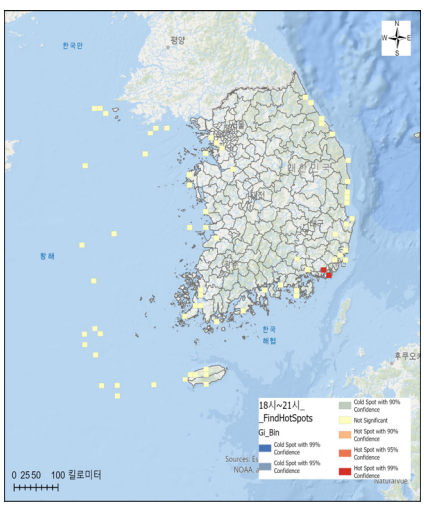
〈그림 4-25〉 시간대별 핫스팟 분석 결과(12시~24시)



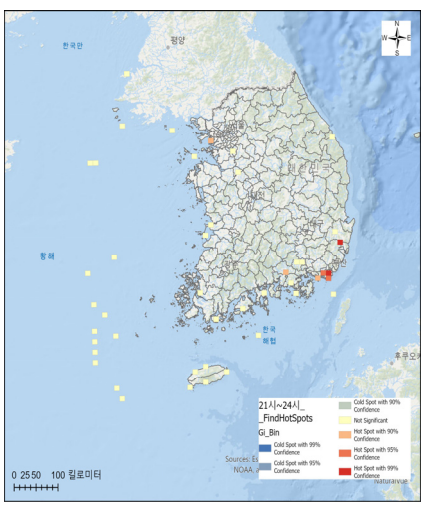
12시~15시



15시~18시



18시~21시



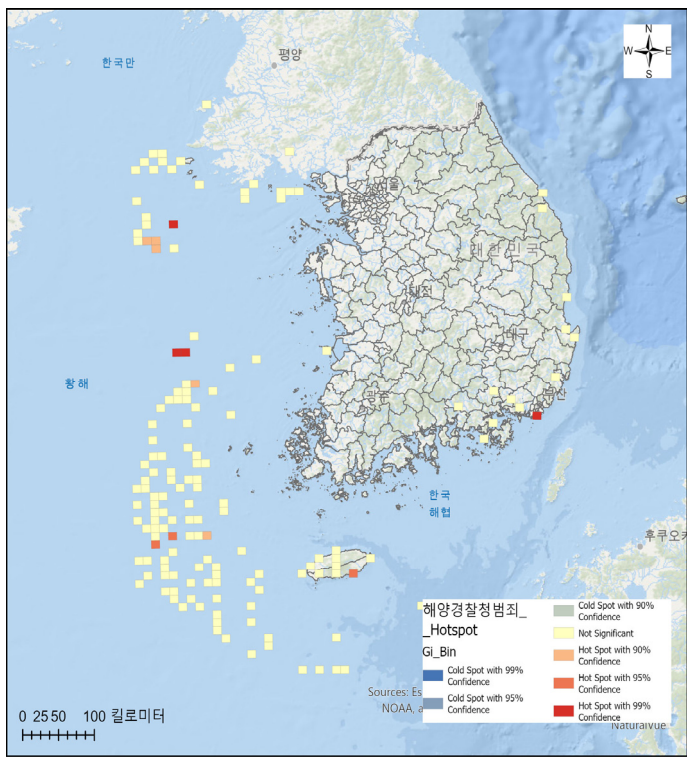
21시~24시

자료: 해양경찰청(2025) 참조하여 저자 작성

(2) 관계기관별 핫스팟 분석

관계기관별 범죄의 핫스팟 분석 결과 해양수산청 관련 범죄의 경우 부산에서 강한 핫스팟을 보이고 있다. 해양경찰청의 경우 부산 일부 지역과 서해에서 핫스팟을 보이며, 범죄 발생이 비교적 먼바다에서 발생하고 있다. 출입국·외국인청의 경우 군산 지역 및 제주 지역에서 핫스팟을 보이고 있다. 지방식품의약품안전청의 경우 목포 지역에서 핫스팟을 보이며, 관세청의 경우 부산 지역에서 핫스팟이 확인된다.

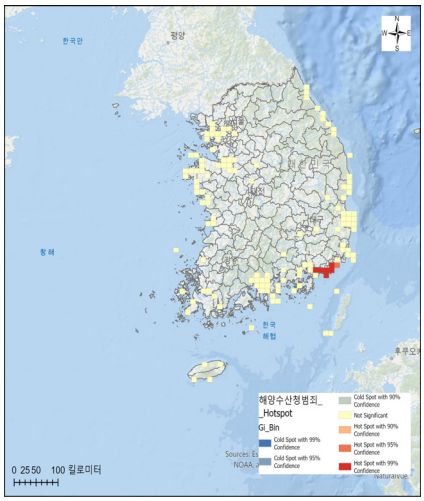
〈그림 4-26〉 기관별 해양 국제범죄 핫스팟 분석 결과(1)



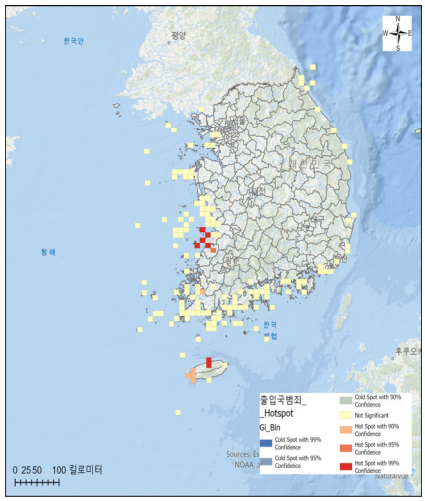
해양경찰청

자료: 해양경찰청(2025) 참조하여 저자 작성

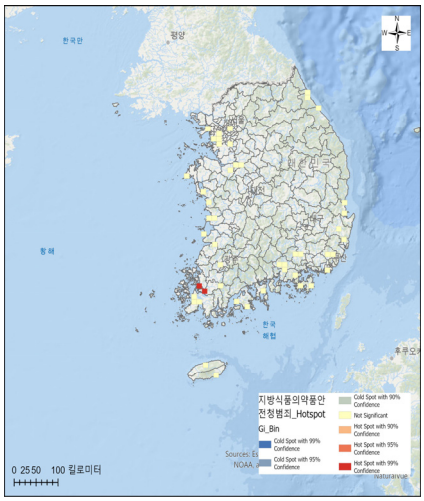
〈그림 4-27〉 기관별 해양 국제범죄 핫스팟 분석 결과(2)



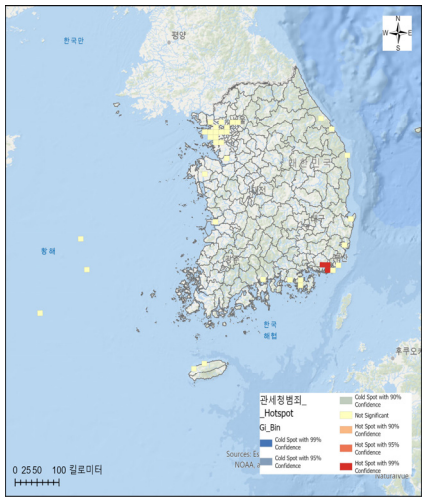
지방해양수산청



출입국·외국인청



지방식품의약품안전청



관세청

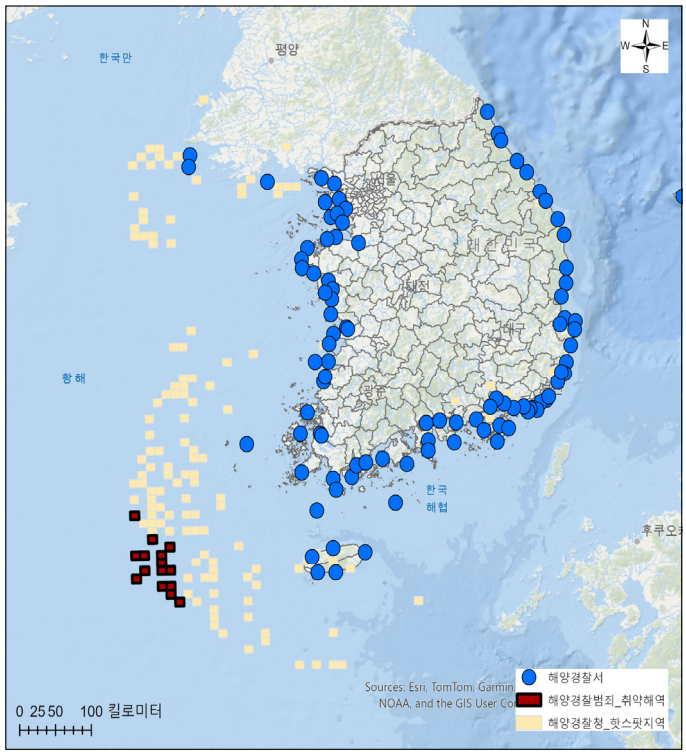
자료: 해양경찰청(2025) 참조하여 저자 작성

(3) 핫스팟 분석 기반 취약 해역 및 지역 도출

관계기관별 국제범죄의 핫스팟 분석 결과를 근거로 범죄 발생 취약 해역 및 지역을 분석하였다. 취약지역은 핫스팟 분석 결과로 도출된 해역들과 관계기관과의 근접성 정보를 기반으로 분석되었다. 각 국제범죄 핫스팟을 기준으로 가장 인접한 관계기관과의 거리 정보를 계산하고, 계산된 거리 정보를 열 개의 분위수로 구분하여 거리가 가장 큰 상위 10%의 해역을 취약지역으로 도출하였다. 취약지역으로 도출된 해역은 국제범죄가 발생하였을 때 인접한 관계기관의 위치가 상대적으로 멀리 위치하여 빠른 조치와 대응이 비교적 어려워 추후 추가적인 조치가 필요함을 시사한다.

지방해양수산청은 육상지역의 핫스팟 지역에는 적절히 분포되어 있으나, 취약지역으로 분석되는 제주 지역 및 도서 지역과는 상대적으로 거리가 먼 것으로 분석되었다. 해양경찰청의 경우 육상지역에서 발생하는 핫스팟은 충분히 대응할 수 있는 수준의 개소가 있으나, 영해 밖 서남해 해상에서 발생하는 범죄의 경우 대응이 어려운 것으로 분석되었다. 출입국·외국인청의 경우 군산 지역에서 범죄가 집중적으로 발생하고 있으나 대응을 위한 적절한 위치에 개소가 위치하고 있으며, 서해 도서해역에서의 취약지역이 발생하고 있다. 지방식품의약품안전청의 경우 관련 범죄 핫스팟이 주로 내륙에서 나타나고 있는데, 강원도 지역 및 제주 지역에서의 취약지역이 나타나는 것으로 분석되었다. 관세청의 경우 육상 개소는 충분한 데 반해, 일부 해상 선박에서 발생하는 범죄의 경우 물리적인 거리로 인해 취약지역으로 분석되었다.

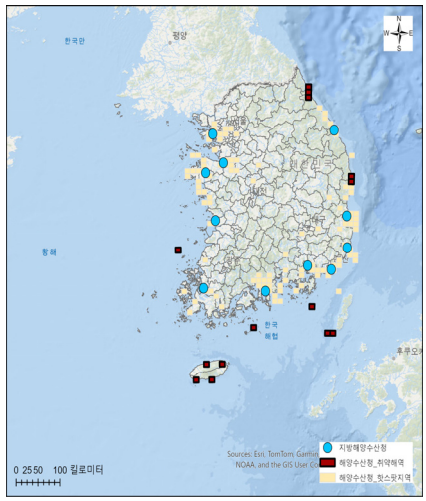
〈그림 4-28〉 기관별 핫스팟 분석 기반 취약 해역 및 지역 분석 결과(1)



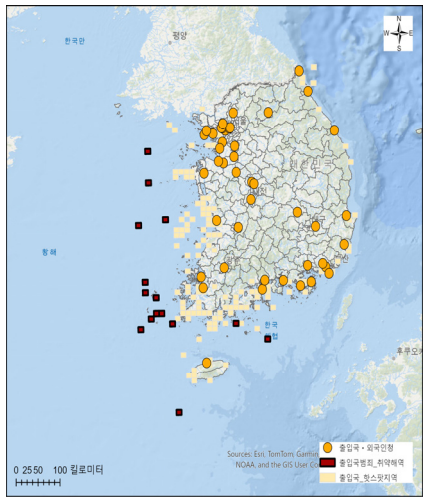
해양경찰청

자료: 해양경찰청(2025) 참조하여 저자 작성

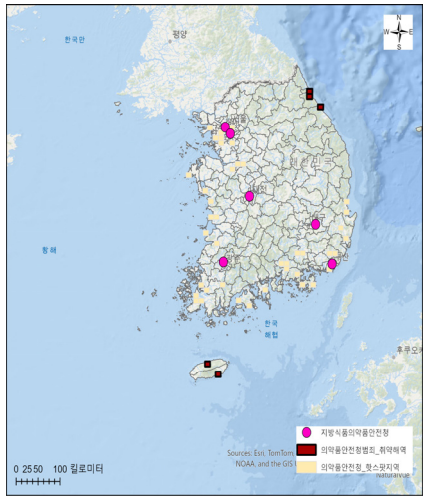
〈그림 4-29〉 기관별 핫스팟 분석 기반 취약 해역 및 지역 분석 결과(2)



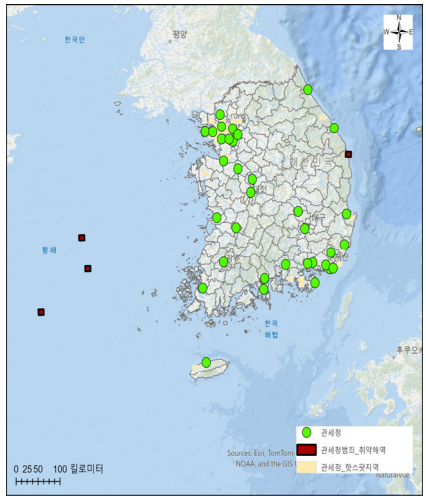
지방해양수산청



출입국·외국인청



지방식품의약품안전청



관세청

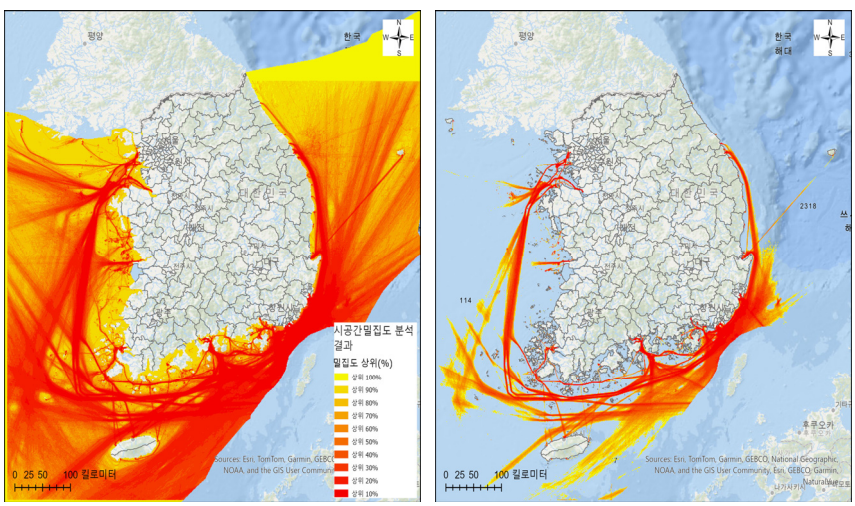
자료: 해양경찰청(2025) 참조하여 저자 작성

(3) 우리나라 해역 해상교통량과 국제범죄 상관분석

해양 국제범죄 중 우리나라 해상교통량과 공간적으로 상관성이 있는 범죄 파악 및 분석을 위해 교통량을 정량적으로 산출하였다. 해상교통량 산출은 GICOMS 시스템을 통해 수집된 AIS 화물선 데이터[291]를 사용하였으며, 유럽 EmodNet에서 수행하고 있는 격자(1km × 1km) 단위의 시공간 밀집도 분석[292]을 활용하였다.

분석 결과는 격자별 선박이 활동한 점유시간(Hour)으로 계산되며, 각 점유시간은 등급화하여 GIS를 통해 표출함으로써 우리나라 주요 선박 교통흐름을 나타낼 수 있다. 본 분석에서는 '20년 1년간의 화물선 AIS 데이터를 활용하였으며,[293] 해상교통량이 많은 해역을 선정하기 위해 격자별 점유시간 기준 등도수 상위 20%의 격자를 추출하였다.

〈그림 4-30〉 우리나라 연안 해상교통량 분석 결과



해상교통량 전체　　해상밀집도 상위 20%

자료: 저자 작성

291) 해양수산부(2025)
292) EMODnet,(2019.3.), pp. 3-7.
293) 해양수산부(2025)

해양 국제범죄 중 해상교통량 상위 20%와 중첩되는 범죄는 총 320건이며, 이 중 발생 건수가 많은 상위 다섯 개 범죄를 조사한 결과, 해양환경관리법 80건, 출입국관리법 73건, 항만지역 등 대기질 개선에 관한 법률 15건, 농수산물의 원산지 표시 등에 관한 법률 14건, 경제수역어업주권법 13건, 기타 125건으로 확인되었다.

상위 다섯 개 범죄의 중첩 건수를 각 범죄의 전체 발생 건수와 비교하여 해상교통량 상위 20% 구간과의 중첩이 범죄 발생에 미치는 상대적 영향성을 분석하였다. 항만지역 등 대기질 개선에 관한 법률 위반은 전 건이 해상교통량 상위 20% 해역에서 발생해 교통량과의 연관성이 가장 높았으며, 해양환경관리법 위반은 75.5%로 그 뒤를 이었다. 농수산물의 원산지 표시 등에 관한 법률과 경제수역어업주권법 위반은 각각 13.6%와 7.0%로, 전체 발생 건수 대비 해상교통량과의 연관성이 상대적으로 낮은 것으로 분석되었다.

〈표 4-13〉 범죄 유형별 발생 건수와 해상교통량 상위 20% 중첩 비율

범죄 유형	전체 발생 건수	중첩 발생 건수	중첩 비율(%)
해양환경관리법	106	80	75.5
출입국관리법	242	73	30.2
항만지역 등 대기질 개선에 관한 법률	15	15	100.0
농수산물의 원산지 표시 등에 관한 법률	103	14	13.6
경제수역어업주권법	185	13	7.0

자료: 저자 작성

반면, 해상에서 해상교통량 상위 20%와 중첩되지 않는 범죄는 총 292건이며, 이 중 발생 건수가 많은 상위 다섯 개 범죄를 조사한 결과, 경제수역어업주권법 165건, 출입국관리법 71건, 영해 및 접속수역법 19건, 외국인 근로자의 고용 등에 관한 법률 여섯 건, 해양환경관리법 네 건, 기타 27건으로 확인되었다.

상위 다섯 개 범죄의 미중첩 건수를 각 범죄의 전체 발생 건수와 비교하여, 해상교통량 상위 20% 구간과의 연관성이 낮은 범죄 유형을 분석하였다. 영해 및 접속수역법 위반은 모든 사례가 교통량 상위 20% 해역 외부에서 발생해 교통량과의 관련성이 가장 낮게 나타났으며, 경제수역어업주권법 위반 역시 89.2%로 상당수 사건이 교통량과 중첩되지 않았다. 출입국관리법 위반은 29.3%로 비교적 낮은 연관성을 보였으며, 외국인 근로자의 고용 등에 관한 법률과 해양환경관리법 위반은 각각 16.2%와 3.8%로 중첩률이 매우 낮은 것으로 나타났다.

〈표 4-14〉 범죄 유형별 발생 건수와 해상교통량 상위 20% 미중첩 비율

범죄 유형	전체 발생 건수	미중첩 발생 건수	미중첩 비율(%)
경제수역어업주권법	185	165	89.2
출입국관리법	242	71	29.3
영해 및 접속수역법	19	19	100.0
외국인 근로자의 고용 등에 관한 법률	37	6	16.2
해양환경관리법	106	4	3.8

자료: 저자 작성

제3절 해양 복합위협 위험성 분석

본 절은 해양 국제범죄의 통계를 통해 확인하기 어려운 해양테러, 해양 사이버위협의 해양 복합위협의 위험성을 해양 국제범죄와 비교하여 우선순위를 도출한다. 특히, 본 절에서는 해양 복합위협 전체 유형에 대한 전문가 설문 응답을 통해 국가적으로 우선적으로 예방, 대비, 대응해야 하는 해양 복합위협을 도출하고 정책적 함의를 도출하고자 한다.

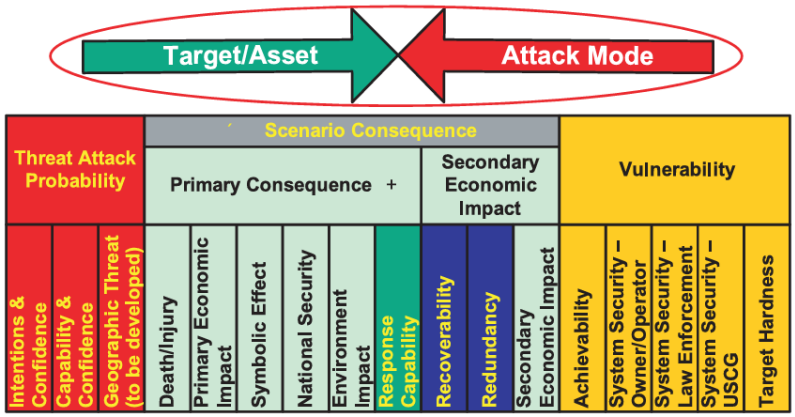
1. 해양위협 위험성 평가 모델(MSRAM)

미국 해안경비대(USCG)는 항만과 해상수송로(SLOC: Sea Lanes of Communication) 등의 주요 해상 인프라에 대한 위협을 체계적으로 평가하고 관리하기 위해 2005년부터 해양안보위험성분석모델(MSRAM, Maritime Security Risk Analysis Model)을 개발하여 적용하고 있다. MSRAM은 9/11 테러 이후 해양사고와 테러 위험에 대응하기 위해 고안된 것으로 국가·지역·현장 수준에서 해양위협과 보안 위험을 체계적으로 평가하고, 도출된 위험을 근거로 관련 자원을 배분하도록 의사결정을 지원하는 평가 모델이다.[294]

MSRAM은 특정 타깃에 대해 여러 공격 수단을 시나리오별로 가정해 '위협 발생가능성(Threat Probability)', '취약성(Vulnerability)', '영향(Consequence)'이라는 세 가지 핵심 평가 요소를 이용해 위험을 산출한다. '위협'은 위협의 의도와 능력, '취약성'은 공격 실현 가능성(Achievability), 시스템 보안(System Security), 대상의 위협 방어 능력(Target Hardness), '영향(Consequence)'은 인명·경제·환경·국가 안보 등 다양한 차원의 부정적 영향으로 세분화된다.

294) Snow Eagle Group(검색일: 2025.9.13.)

〈그림 4-31〉 USCG MSRAM 평가 모델



자료: Downs(2008)

이에 본 연구에서도 MSRAM의 위험성 평가 모델을 활용하여 본 연구의 대상이 되는 해양 복합위협 유형의 위험성을 평가하고자 한다. 다만, MSRAM의 위험성 평가는 개별 위협 대상 또는 지역을 선정하여 이들에 대한 개별 위험성을 평가하여 해당 지역 또는 대상을 보호하기 위한 자원 배분, 위협 억제 정책 등 의사결정 과정에 MSRAM을 활용한다. 특히, 위협 발생가능성, 취약성, 영향으로 대표되는 요소들을 평가하기 위해, 의도 등을 제외한 대부분의 요소를 사망, 경제적 피해 등 사회 인구학적 통계, 기술 개발 수준, 공격 수단, 방어 수단, 대응 시스템 등을 수치화하고 정량화하여 객관적인 평가를 시도하고 있다. MSRAM은 또한 보호 대상과 또는 위협 대상을 분류하고 이러한 대상에 따른 위협 또는 공격 수단을 구분하여 관련 대상에 대해 발생가능성이 높은 위협 수단을 평가하여 이에 대응하기 위한 전략 및 대응 방안 수립하는 데 객관적 위협 지수를 제공한다. 다만 본 연구에서는 해양 복합위협으로 분류하고 있는 해양 국제범죄, 해양테러, 해양 사이버위협과 관련하여 해양 국제범죄를 제외하고 객관적인

발생 통계, 기술 개발 척도, 공격 수단, 방어 수단, 대응 시스템 등에 관한 수치화한 데이터를 확보하기 어렵고 위협에 관한 분류체계가 MSRAM과 상이하여 위험성 평가를 위한 해양 복합위협의 유형을 〈표 4-15〉와 같이 분류하여 개별 위협에 대한 위험성을 전문가 설문지 응답을 통해 평가하고자 한다.

〈표 4-15〉 해양 복합위협 유형, MSRAM 공격 수단, 해양 국제범죄 유형

해양 복합위협 분류		USCG MSRAM	해양 국제범죄 및 해양범죄 유형	
해양 국제 범죄	밀입(출)국	Transfer of Terrorist	출입국문란	밀입국
				무사증
				무단이탈
				밀항
				밀출국
	밀수(출)입	Transfer of weapons/materials	밀수입·출	밀수입
				밀수출
	밀수(출)입	Transfer of weapons/materials	국익·산업보호	해양산업기술보호
				지적재산 침해
				불법위폐,외국환거래
			국민사회안전	원산지 허위표시
				불량식품범죄
				안전불감 범죄
				마약류 범죄
	납치	Hostage Taking	인권보호	인권침해
		Hijacking of Vessel		외국인권익침해
	해적 및 무장 강도	Attack by Hijacked Vessel	인권보호	인권침해
		Attack by Hijacked Large Aircraft		

해양 복합위협 분류		USCG MSRAM	해양 국제범죄 및 해양범죄 유형	
해양 테러	해양테러(연안 주요시설(발전소, 주요 항만 등) 공격, 다중이용시설(여객선, 여객터미널 등) 공격 등)	Boat Bomb	해양테러*	해양테러
		Boat Bomb(While vessel is present)		
		Passenger/passerby Explosives/Improvised Explosive Devices		
		Sabotage		
		Car/Truck Bomb		
	드론 공격	Standoff Weapon Launched from Water and Land(including Man-Portable Air Defense Weapon)	국민사회안전	안전불감 범죄
		Small Suicide Aircraft Attack		
	해저시설 공격	Swimmer/Diver/Underwater Delivery Systems	국민사회안전	안전불감 범죄
		Mines(Aquatic)		
	대량살상무기	Chemical, Biological, Radiological, Nuclear	환경보존	외국선박 환경오염
해양 사이버 위협	사이버 공격	Cyber Attack	해양 사이버범죄**	해양 사이버범죄
기타	기타	Ability to add additional DOD Attack modes as necessary	출입국문란	불법체류·취업
			기타	기타 범죄

주: *관련 통계는 대외비로 별도 관리
**해양 사이버범죄는 해양 범죄 통계에 포함하여 산정되고 있어 국제범죄가 아닌 일반 수사범죄로 분류
자료: US Government Accountability Office(2011), p. 11; 해양경찰청(2025) 등을 참조하여 저자 작성

이는 현재 제도상 정형화 되어 있지 않은 해양 복합위협을 최근 발생 동향과 사회적 영향 등을 고려하여 도출하고 이를 근거로 향후 미래에 대응해야 하는 위협성을 시범적으로 평가하기 위한 것이다. 이에 보다 객관적

인 위험성 도출을 위해서는 향후 정량화된 사회인구학적 데이터 개별 위협 요소 및 공격 수단에 대한 기술적 정보, 위협 실현 수단, 발생 지역의 시스템 보안 정보 등을 확보하여 계량화하고 이를 구체화된 위험성 평가 모델에 대입하여 산출하는 것이 필요하다.

2. 해양위협 위험성 평가 결과

MSRAM의 평가 방법을 기반하여 본 연구 또한 해양 복합위협의 위험성을 평가하기 위해 위협 발생가능성(Threat Probability)', '취약성(Vulnerability)', '영향(Consequence)'에 대한 전문가 평가를 실시하고 각 요소에 대한 평갓값을 곱하여 위험성 평가 지수를 산출한다.

〈그림 4-32〉 해양 복합위협 위험성 평가 모델



자료: 저자 작성

특히, 개별 평가 요소인 '위협 발생가능성'은 의도와 능력으로, '취약성'은 실행(실현) 가능성, 정부 보안 체계 역량, 위협 대상의 방어 능력으로, '영향'은 인명 피해 정도, 재산 피해 정도, 국가 안보 영향, 환경 피해, 사회적 영향으로 세분화하여 평가하고 그 평갓값의 합을 개별 지수에 대한 결괏값으로 도출한다.[295]

295) 개별 지수에 대한 평가 기준 및 척도 등에 대한 보다 상세한 전문가 설문 사항은 부록을 참고

1) 해양 복합위협의 위험성 우선순위

위험성 평가 설문지를 통해 구체적으로 유형화한 해양 복합위협에 대한 위험성을 평가한 결과, 해양 사이버위협의 위험도가 가장 높은 것으로 확인되었다. 다음으로 드론 등 무인체계를 활용한 새로운 위협에 대한 위험도가 높은 것으로 확인되었다.

〈표 4-16〉 해양 복합위협 위험성 순위

해양 복합위협 분류		산출지수	위험도 순위
해양 국제범죄	밀입(출)국	37,877,640	7
	밀수(출)입	40,327,785	6
	납치	19,084,320	8
	해적 및 무장강도	18,588,042	9
해양테러	해양테러*	42,036,155	4
	드론 공격	49,470,700	2
	해저시설 공격	42,716,520	3
	대량살상무기	41,251,392	5
해양 사이버위협	사이버 공격	51,268,728	1
기타	기타	1,941,966	10

주: 연안 주요시설(발전소, 주요 항만 등) 공격, 다중이용시설(여객선, 여객터미널 등) 공격 등
자료: 저자 작성

이는 제2장의 복합위협의 사례에서 검토한 바와 같이 최근 국제적으로 해양 사이버위협과 무인수상정 등 무인체계를 이용한 위협이 국제적으로 증가하고 있는 반면, 국내적으로 이러한 위협에 대응하기 위한 체계, 장비, 시설, 제도 등이 미흡하기 때문인 것으로 판단된다. 이에, 향후 이러한 위협의 위험성을 중심으로 국내에서 발생 가능한 구체적인 위협을 시나리오 내지 사례를 중심으로 분석하고 이에 대응하기 위한 기관별 협력체계, 제도, 시설 및 장비 등에 대한 정책 개발이 필요한 것으로 사료된다.

2) 발생가능성, 취약성, 영향에 따른 우선순위

개별 평가 요소에 대한 결과를 분석하면, 먼저 해양 복합위협 중 가장 발생가능성이 높은 것은 해양 국제범죄 중 밀입(출)국과 밀수(출)입으로 나타났다. 다음으로 해양 사이버위협의 발생가능성이 높은 것으로 나타났다. 최근 우리나라 국가 경제의 선진국 진입과 코로나 팬데믹 이후 국경 개방으로 밀입(출)국에 대한 수요가 증가하고, 이를 지원하는 국내외 조직 및 인프라가 조성되어 향후 출입국 사범 위협이 증가할 것으로 예상되기에 이러한 위협의 우선순위가 높은 것으로 분석된다. 또한 우리나라는 최근까지 마약청정국 지위를 유지하고 밀수 거래가 어려운 국가로 여겨지고 있었으나, 요트 등 레저 선박 이용의 증가와 함께 세관 및 검역이 다소 완화된 선박 및 항만을 통해 불법 무기 등의 밀수 사례가 적발되고 있으며, 우리나라를 중간유통 지점으로 대량의 마약을 아시아로 유통하는 사례가 증가하고 있어 이에 대한 위협도 증가하고 있는 것으로 분석된다. 다음으로 사이버위협에 대해서는 항만시설, 해운물류시스템 등에 대한 해킹 사례가 최근 증가하고 있는 반면, 해양수산부의 사이버보안 지침을 제외하고 이에 효과적으로 대응하기 위한 구체적인 정책 및 수단이 미흡하여 이러한 위협의 미래 발생가능성이 높은 것으로 분석된다.

〈표 4-17〉 해양 복합위협 발생가능성 순위

해양 복합위협 분류		산출지수	순위
해양 국제범죄	밀입(출)국	285	1
	밀수(출)입	285	1
	납치	174	8
	해적 및 무장강도	162	9
해양테러	해양테러*	217	5
	드론 공격	230	4
	해저시설 공격	201	6
	대량살상무기	192	7

해양 복합위협 분류		산출지수	순위
해양 사이버위협	사이버 공격	258	3
기타	기타	86	10

주: 연안 주요시설(발전소, 주요 항만 등) 공격, 다중이용시설(여객선, 여객터미널 등) 공격 등
자료: 저자 작성

다음으로 해양 복합위협 중 취약성이 가장 높은 것은 해양 사이버위협으로 나타났으며, 다음으로 취약성이 높은 것은 해저시설 공격으로 확인된다. 드론 공격 등 무인체계를 이용한 해양 복합위협에 대한 취약성 또한 높은 것으로 확인되었다. 이들은 주로 해양 복합위협 중 새로운 형태의 위협으로 과거에 주로 확인되지 않았던 위협이다. 특히, 무인수상정 및 드론 공격 등 무인체계를 이용한 해양 복합위협은 해양 사이버위협과 연계하여 복합적으로 나타나기 쉬우며, 러시아-우크라이나 전쟁, 이스라엘-중동 전쟁 등을 통해 이미 그 피해와 영향이 막대한 것으로 확인되었다. 예를 들어, 홍해에서 후티 반군이 서방국가들의 선박을 무인수상정을 통해 공격하는 행위는 글로벌 공급망을 마비시키거나 물류비용을 증가시키는 것으로 분석되고 있다. 또한 해저시설 공격은 최근 한·중 해저케이블 손상, 대만 해저케이블 훼손 사건, 일본 해저 통신 케이블의 도청 사건 등을 통해 국제 금융 통신 마비, 국가전략 정보의 누수 등으로 국가 안보와 기능에 직접적인 영향 미칠 수 있는 것으로 확인되었다. 특히, 이러한 위협은 관할 해역의 이상 행동 내지 활동을 상시적으로 감시하는 체계와 온라인 활동을 감시하는 정보공유체계가 구축되어 있지 않고는 행위자의 위협을 예방하거나 대응하기가 쉽지 않다. 반면, 우리나라의 경우, 사이버안보 등 육상 시설 및 국가주요시설에 대한 대응 협력체계는 구축되어 있으나, 항만 등 주요 해양시설의 해킹과 해상 무인체계 활용 위협에 대해서는 제도 및 체계적 대응이 미흡한 것으로 판단된다. 이에 따라, 국내적으로 해양 사이버위협, 해저시

설 공격 등 신흥 해양 복합위협에 대한 취약성이 높은 것으로 분석되었다.

〈표 4-18〉 해양 복합위협 취약성 순위

해양 복합위협 분류		산출지수	순위
해양 국제범죄	밀입(출)국	296	5
	밀수(출)입	303	4
	납치	240	8
	해적 및 무장강도	209	9
해양테러	해양테러*	265	7
	드론 공격	314	3
	해저시설 공격	322	2
	대량살상무기	273	6
해양 사이버위협	사이버 공격	329	1
기타	기타	117	10

주: 연안 주요시설(발전소, 주요 항만 등) 공격, 다중이용시설(여객선, 여객터미널 등) 공격 등
자료: 저자 작성

마지막으로 해양 복합위협의 영향력 지수는 대량살상무기를 통한 공격이 가장 높은 것으로 확인되었다. 다음으로 해양테러와 드론 공격 등 무인체계를 활용한 공격의 영향력이 높은 것으로 확인되었다. 이는 위협의 물리적 피해가 높고 인명 피해가 막대한 위협을 중심으로 영향력이 높은 것으로 평가되었다. 주목할 만한 점은 드론 공격 등 무인체계를 통한 위협이 마약 밀수 등을 포함한 밀수(출)입 위협보다 그 영향력이 상대적으로 높게 평가된 것이다. 이는 무인수상정 등 무인체계 기술이 최근 급격히 발전하고 있고, 일반 대중에 대한 기술의 접근성 또한 용이해 위협의 발생가능성이 높기 때문인 것으로 판단된다. 특히, 최근 국제 정세를 고려할 때, 무인수상정 등을 원거리에서 조정하여 해상교량, 해안발전소, 상선 등 해양 주요시설 및 대상을 공격하는 사례를 쉽게 확인할 수 있는 반면, 행위 주체자

가 원거리에 위치하고 있어 행위의 즉각적인 확인이 어렵고, 국가적 차원에서 대응 방안 또한 마련이 쉽지 않기 때문에 이러한 위협의 영향이 상대적으로 높은 것으로 분석된다.

〈표 4-19〉 해양 복합위협 영향 순위

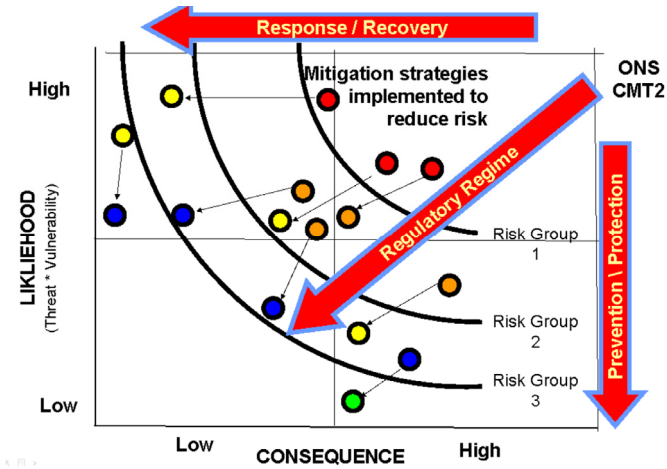
해양 복합위협 분류		산출지수	순위
해양 국제범죄	밀입(출)국	449	9
	밀수(출)입	467	7
	납치	457	8
	해적 및 무장강도	549	6
해양테러	해양테러*	731	2
	드론 공격	685	3
	해저시설 공격	660	4
	대량살상무기	787	1
해양 사이버위협	사이버 공격	604	5
기타	기타	193	10

주: 연안 주요시설(발전소, 주요 항만 등) 공격, 다중이용시설(여객선, 여객터미널 등) 공격 등
자료: 저자 작성

3) 해양 복합위협 위험성 분석

미 USCG의 MSRAM은 위험성 평가 결과에 따라 대상 및 위협의 우선순위를 대응 및 복구(Response/Recovery), 제도적 대응(Regulatory Regime), 예방 및 대비(Prevention/Protection)) 등으로 대응 방향을 구분하여 분석한다. 분석을 위해 발생가능성 및 취약성과 영향을 기준으로 산점도를 작성하고 관련 정책의 방향성을 설정한다.

〈그림 4-33〉 USCG MSRAM 위험성 분석 모델 및 정책 대응 방향

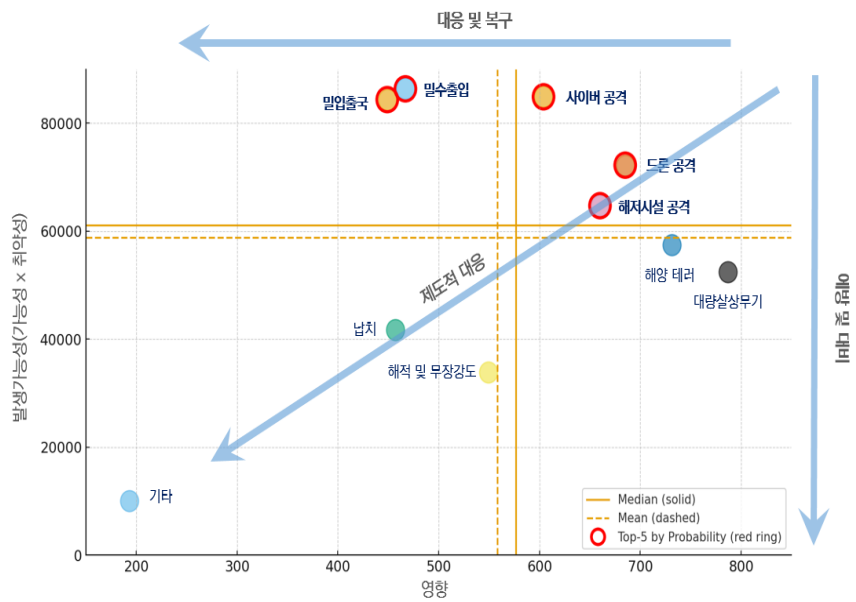


자료: Downs(2008)

이러한 MSRAM의 분석 모델에 따라 본 절에서 실시한 위험성 전문가 설문조사를 통한 해양 복합위협의 위험성을 분석하면 다음과 같다. 먼저, 드론 공격, 해저시설 공격, 사이버위협 등 신흥 해양 복합위협에 대해서는 예방, 대비, 대응, 복구 등 위협 대응 전 주기에 걸친 대응 정책 및 제도적 수단이 마련되어야 하는 것으로 분석되었다. 또한, 밀입(출)국 및 밀수(출)입에 대해서는 예방 및 대비를 위한 정책이 우선적으로 마련되어야 하는 것으로 분석되었다. 특히, 신흥 복합위협의 경우, 제2장 사례 분석과 제3장 국외 제도 분석에서 확인할 수 있듯이, 하나의 개별 기관의 대응보다, 국가 자원 및 기능에 따라 범부처 협력체계를 통한 통합적 국가적 대응체계가 마련되어야 하는 것으로 판단된다. 또한 이러한 위협은 일단 발생하면 국가 안보와 국익 전체를 위험에 빠뜨릴 수 있어 이에 대응하기 위한 국가 차원의 전략 체계 또한 마련되어야 하는 것으로 판단된다. 밀입(출)국 및 밀수(출)입의 경우, 일부 위협 유형에 대해서는 협의체가 구성되어 있으나,

이를 포괄적으로 예방 및 대비하기 위한 협력체계가 부족한 것으로 판단된다. 즉, 밀입(출)국 및 밀수(출)입의 효과적 예방 및 대비를 위해서는 이들 위협에 대한 상시적인 감시와 기관 간 정보 공유 체계가 필수적인 반면, 국내적으로 기관 간 상시적인 정보 공유 및 분석 체계는 미흡한 것으로 판단된다. 이에, 이들 위협을 효과적인 대응을 위해서 위협에 대한 상시 감시 체계를 보완하는 한편, 이들 위협의 흐름에 대한 정보를 기관 간 공유하는 것이 필요하다.

〈그림 4-34〉 해양 복합위협 위험성 분석



자료: 저자 작성

제4절 국내 대응체계 한계 및 데이터 분석 시사점

1. 분절적 대응체계 및 책임의 모호성

본 장은 국내 대응체계를 해양 복합위협의 유형별로 살펴보고, 앞서 검토한 국외 대응체계와의 비교를 통해 개선 사항을 도출하였다. 우선, 본 연구는 해양 국제범죄에 대한 국내 대응체계가 관할 및 대상별로 단속과 처리의 책임·권한이 기관별로 분산되어 운영되고 있음을 확인하였다. 이로 인해 위협에 대한 연속적이고 효과적인 대응에 한계가 존재하는 것으로 분석된다. 이는 국외의 경우 해양 위협에 대해 일원화된 혹은 통합적 대응을 시도하는 것과 달리, 국내에서는 동일한 위협 행위에 대해 여러 기관이 각자의 관할에 따라 요청 시 단절적으로 대응하는 구조로 운영되고 있음을 의미한다. 예를 들어, 육상에서 항만을 거쳐 선박을 이용해 국외로 밀항하는 사례의 경우, 위협 행위가 발생하는 공간적 범위에 따라 대응기관이 출입국·외국인청(육상) → 해양수산부(항만공사, 항만) → 해양경찰청(항계 밖 해상)으로 순차적으로 변경된다. 이러한 상황에서 사건의 인계나 기관 간 역할 전환 및 협조가 시의적절하게 이루어지지 않을 경우, 대응 공백이나 사각지대가 발생하여 결국 위협의 최종 실현으로 이어질 수 있다.

또한 권한의 분산은 관할 전환 시점에서 기관 간 권한의 중첩을 초래할 가능성이 있으며, 이는 나아가 책임 회피로 연결될 위험도 존재한다. 예컨대, 항만 수상구역에서의 해양경찰 단속 권한, 해양수산부 또는 항만공사의 보안관리 권한, 연안 지역에서의 출입국·외국인청의 단속 권한과 해양경찰의 밀입국자 단속 권한이 일부 동일 구역에서 중복되어 있다. 이러한 권한 중첩은 사건에 따라 기관 간의 공조나 협력이 개별적 재량에 의해 이루어질 수밖에 없게 되며, 결과적으로 책임 회피로 이어질 가능성을 내포한다.

따라서 기관 간 협조를 임의적 수준이 아닌 제도적으로 규정하여, 유기적 협력 체계가 지속적으로 작동하도록 해야 한다. 결국, 권한과 책임의 분산에서 비롯되는 한계를 극복하기 위해서는 위협의 효과적 대응을 위한 통합적 대응체계의 구축이 필요하다. 이를 통해 관련 기관의 권한과 기능을 상시적으로 조정할 수 있도록 하고, 특히 관할 및 대상에 따른 기관별 권한과 책임을 지침 등의 형태로 제도화하여 유기적 협력과 공조가 가능하도록 해야 한다.

한편, 해양 국제범죄 대응체계와는 달리 해양테러 및 해양 사이버위협에 관한 국내 대응체계는 상대적으로 통합적 접근을 시도하고 있는 것으로 보인다. 다만, 현행 해양테러 및 국가 사이버위협 대응체계는 국가행위자의 회색지대 위협, 해저케이블 훼손, 무인체계 활용 공격 등 신흥 해양 복합위협에 대응하는 데 한계가 있다. 특히, 「테러방지법」은 해양테러의 정의와 범위를 별도로 규정하지 않고 있어, 해양에서 시작되어 육상 주요시설 공격으로 이어지는 테러 행위의 경우 어느 기관이 주관하여 대응해야 하는지 역할이 불명확할 수 있다. 또한 국가 사이버안보 체계 내에서 해양 분야의 주무 부처가 해양수산부로 명시되어 있기는 하나, 이는 주로 해사·항만 분야의 사이버보안 강화 정책에 한정되어 있다. 즉, 자율운항시스템, 항만시스템 해킹 등 해양 사이버범죄 대응에 관한 요소는 현 체계에서 누락되어 있으며, 이를 보완하기 위한 정책적 개발과 기관 간 협력이 필요함이 확인되었다.

본 장은 이러한 국내 대응체계의 취약점과 개선사항을 토대로, 우선적으로 대응해야 할 해양 복합위협을 확인하기 위해 해양 국제범죄 통계의 변동성과 시계열 분석을 수행하였다. 아울러 대응기관의 위치와 범죄 발생 간 관계를 확인하기 위해 GIS 분석을 실시하였고, 향후 국내 관할 해역에서 우선 대응이 필요한 해양 복합위협을 도출하기 위한 위험성 분석도 병행하였다.

먼저 해양 국제범죄 통계의 변동성 분석 결과, 우리 해역에서 가장 우선적으로 대응해야 할 위협은 밀입(출)국 및 밀항 등과 관련된 출입국문란 범죄, 그리고 밀수(출)입 등 관세범죄인 것으로 나타났다. 이러한 범죄에 대응하기 위해 단기적으로는 범죄 발생의 원인 분석과 국가 자원의 효과적 활용을 통해 사건 발생을 억제·관리하는 노력이 필요하다. 장기적으로는 범죄의 변동성을 지속적으로 관리·대응하기 위해 범죄의 경향, 동향, 원인을 다층적으로 분석하고 이에 기반한 대응조직 및 자원 배분 등 정책적 대응 방안을 수립할 필요가 있다.

또한 GIS 분석 결과, 해양 국제범죄의 관리 및 대응 과정에서 정보 공유의 부족, 해상 및 도서 지역 등 원거리 범죄 대응 자원의 부족, 복합위협 발생의 불확실성이 확인되었다. 분석은 지난 5년(2021년~2024년)간 해양경찰청 통계에 기반하여 범죄 발생 핫스팟, 기관 위치와 범죄 발생 위치 간의 상관관계, 해상교통량과 범죄 발생 간의 관계를 중심으로 이루어졌다. 특히 범죄 발생 핫스팟 및 위치 분석을 통해 범죄 유형에 따라 관련 기관 간 협력이 범죄 예방과 대응에 필수적임을 확인하였다. 구체적으로, 해양수산부와 관련된 보안사고는 주로 부산 지역에서 발생하였고, 출입국 사범 등 출입국·외국인청 관할 범죄는 군산 및 제주 등 서해와 제주 먼바다에서 집중되었다. 또한 식품안전 사범 등 지방식품의약품안전청 관련 범죄는 주로 목포 등 섬 지역, 마약 밀수 사범 등 관세청 관련 범죄는 부산 지역에서 주로 발생한 것으로 분석되었다. 결론적으로 핫스팟 분석 기반으로 취약해역 및 지역을 도출한 결과 관할기관별로 취약지역이 상이하고 넓게 분포되어 있어 통합적 관리의 필요성을 확인할 수 있다. 해양경찰청의 취약지역은 남서쪽 해안에서 멀리 떨어진 곳이며, 출입국·외국인청과 관세청은 서해안 지역에 넓게 분포하고 있어 개별기관에서 담당하기에는 어려운 측면이 존재한다. 특히 해양경찰과 같이 연근해 지역을 넓게 담당할 수 있는 기관이 아닌 출입국·외국인청과 관세청이 원거리 해역을 관할하는 것은 현

실적인 어려움이 존재한다. 지방해양수산청과 지방식품의약품안전청은 제주도와 동해안 지역에 일부 유사한 취약지역이 존재하여 상호 통합관리 가능성이 존재하는 것으로 확인된다.

해양 국제범죄 유형에 따라 발생 위치가 상이하고, 최종 처분 기관을 달리하고 있어 이를 통합적으로 관리하는 체계가 필요함을 확인할 수 있다. 특히, 해양경찰청의 경우, 발생하는 이들 모든 위협에 대해 일반사법경찰기관으로 초동 조치를 취해야 하는 의무와 책임을 가지고 있다. 또한, 해양경찰청은 해상에서 실효적으로 단속할 수 있는 유일한 능력과 자원을 가지고 있는 기관으로 관계기관과의 정보 및 첩보에 대한 협력체계가 필수적으로 구축되어야 함을 확인할 수 있었다. 또한 본 연구는 해상교통량과 범죄 발생 위치와의 분석을 통해, 제2장의 해양 복합위협의 불확실성이 우리나라 관할 해역에서도 나타남을 확인할 수 있었다. 즉, 사고 등 우발적으로 발생하는 해양환경 오염 범죄를 제외하고 대다수의 범죄가 일반적인 해상교통의 흐름에서 벗어나서 발생하는 것을 확인할 수 있었다. 이에 해양 국제범죄의 효과적인 대응을 위해서는 민·관·군·경 등의 자산을 통합적으로 활용하여 위협을 협력적으로 관리하는 범정부 체계가 필요하다는 것을 확인할 수 있었다.

2. 데이터 분석에 따른 정책 우선순위

본 장에서는 미래 해양 복합위협 분석을 위해 위협에 대한 전문가 설문 및 자문을 통해 향후 우리나라 관할 해역에서 발생 가능한 위협의 위험성을 분석하고 이에 대한 정책적 시사점 또한 도출했다. 먼저, 해양 복합위협 위험성 분석을 기준으로 드론 공격, 해저시설 공격, 사이버위협 등 신흥 해양 복합위협에 대한 위협 대응 전 주기에 걸친 대응 정책 및 제도적 수단이

마련되어야 하는 것으로 분석되었다. 밀입(출)국 및 밀수(출)입에 대해서도 예방 및 대비를 위한 정책이 우선적으로 마련되어야 하는 것으로 분석되었다. 특히, 신흥 복합위협의 경우, 제2장의 사례와 제3장의 국외 사례에서도 확인하였듯, 하나의 개별 기관의 대응보다, 국가 자원 및 기능에 따라 범부처 협력체계를 통한 통합적 국가적 대응체계가 마련되어야 하는 것으로 판단된다. 또한 이러한 위협은 일단 발생하면 국가 안보와 국익 전체를 위험에 빠뜨릴 수 있어 이에 대응하기 위한 국가 차원의 전략 체계 또한 마련되어야 하는 것으로 판단된다. 밀입(출)국 및 밀수(출)입의 경우, 일부 위협 유형에 대해서는 협의체가 구성되어 있으나, 이를 포괄적으로 예방 및 대비하기 위한 협력체계가 부족한 것으로 판단된다. 즉, 밀입(출)국 및 밀수(출)입의 효과적 예방 및 대비를 위해서는 이들 위협에 대한 상시적인 감시와 기관 간 정보 공유 체계가 필수적인 반면, 국내적으로 기관 간 상시적인 정보 공유 및 분석 체계는 미흡한 것으로 판단된다. 이에, 이들 위협에 대한 효과적인 대응을 위해서 위협에 대한 상시 감시체계를 보완하는 한편 이들 위협의 흐름에 대한 정보를 기관 간 공유하는 것이 필요한 것을 확인할 수 있었다.

05
해양 복합위협의 실효적 대응 방안

제1절 해양 복합위협의 실효적 대응을 위한 정책 방향

해양 복합위협은 제2장에서 분석한 바와 같이 4차 산업기술의 발달과 함께 사이버, 무인체계를 결합한 복합적인 형태로 나타나는 위협으로 그 대상과 형태가 점차 확대되고 있다. 이에 제3장에서 살펴본 바와 같이 주요 선진국들은 변화하고 있는 해양 복합위협에 효과적으로 대응하기 위해 단일 부처 내에 해양경비를 비롯해 해양에서 발생하는 다양한 위협에 대응하도록 체계를 구축하고 있다. 특히, 미국은 USCG, 세관국경보호청, 이민세관단속국 등 해양 복합위협에 대응하는 주요 기관들을 국토안보부 예하에 두고 위험성 평가부터, 관련 정책 수립, 국가 자원 배분, 대응 수단 확보, 현장 대응 등 위협의 예방부터 대응까지 하나의 부처 내에서 유기적으로 협력하여 실행할 수 있도록 대응체계를 형성하고 있다. 일본 또한 해양 복합위협의 정보 수집부터 대응 및 수사까지 해상보안청에서 대응 업무를 전담하여 효율적이면서 효과적인 위협 대응을 위한 체계를 구축하고 있다. 영국은 다양한 기관에서 그 역할에 따라 해양 복합위협에 대응하지만 다부처가 일련의 구분된 책임에 따라 일원화된 플랫폼인 합동해양안보센터를 통해 관련 정보와 상황을 공유하고 유기적으로 협력하고 있다. 영국의 이

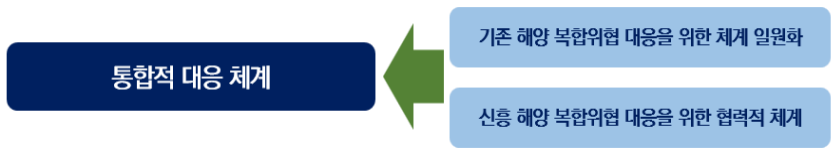
러한 협력적 플랫폼은 EU의 유럽복합위협대응센터에서도 확인할 수 있다.

반면 제4장에서 살펴본 바와 같이 국내 대응체계는 기관의 관할(사물 및 지역)에 따라 그 책임과 역할이 분산되어 있으나, 위협 대응을 위한 협력체계가 미흡하여 위협의 대응이 파편적으로 이루어지고 있다. 뿐만 아니라, 일부 관할에 대해서는 역할 및 기능의 중첩이 발생하거나 대응 자원의 부족으로 기관 간 필수적인 협력이 이루어져야 하나, 책임에 관한 제도가 명시적으로 갖추어져 있지 않다. 즉, 지속적으로 발생하고 있는 해양 국제범죄는 마약류 범죄 대응을 위한 대책협의회를 제외하고 밀입(출)국, 밀수(출)입, 해적 및 무장강도, 납치 및 인신매매, 불법조업, 해양오염 등 개별 위협에 대해 각 기관이 그 대상과 관할 범위에 따라 분절적으로 대응한다. 협력체계 또한 운영에 있어서 해양경찰청, 관세청, 출입국·외국인청 등이 협력양해 각서(MoU)를 체결하고 운영하고 있으나, 이는 위협의 포괄적 대응보다 마약 등 주요 위협에 대해 제한적 정보 공유 내지 자원 협력을 시도할 뿐이다. 뿐만 아니라, 해양 복합위협의 가장 주요한 수단이 되는 해양 사이버위협 관련해서는 해양수산부와 해양경찰청이 해사 사이버안전과 해양 사이버범죄를 구분하여 대응하고 있으나, 대응하고자 하는 대상이 상호 연관될 수 있어 그 경계가 모호하다. 마지막으로 해저시설 공격 및 드론 공격 등 신흥 해양 복합위협에 대해서는 국외 사례를 통해 지속적인 위험성이 증가할 것으로 예상되나, 국가적인 대응체계 내지 기관별 협력체계가 여전히 미흡한 것으로 판단된다. 또한 이들 위협은 단일의 사건으로 국익 및 국가 안보에 막대한 영향을 미칠 수 있으므로 국가 차원의 전략적 대응이 요구되나 이에 대한 준비 또한 부족한 것으로 판단된다.

따라서 해양 복합위협에 효과적으로 대응하기 위해서는 첫째로, 현재 분절적으로 운영되고 있는 국내 대응체계를 개선하고, 범부처를 통한 통합적 대응체계가 구축되어야 할 것으로 판단된다. 통합적 대응이란 기존의 기관 간 분절화된 체계를 일원화하고, 동시에 대응체계가 미흡한 신흥 위협에

대해서는 법집행기관을 중심으로 포괄적 협력이 이루어질 수 있도록 구조화하는 것을 의미한다. 이는 책임의 경계가 모호한 해양 복합위협에 효과적으로 대응할 수 있도록 기관 간 기능과 역할을 조정하여 책임을 명확히 하고 한정된 자원을 효율적으로 운영하여 발생하는 위협에 실질적으로 대응할 수 있는 대응체계 마련을 의미한다.

〈그림 5-1〉 해양 복합위협 통합적 대응체계



자료: 저자 작성

둘째, 신흥 해양 복합위협으로부터 국익과 해양안보를 효과적으로 확보하기 위해서는 해양 복합위협에 효과적으로 대응하기 위한 국가전략이 수립되어야 할 것으로 판단된다. 제2장의 사례 분석에서도 확인할 수 있듯이 신흥 해양 복합위협은 단 한 차례의 발생만으로도 글로벌 공급망의 위기나 국가 이익의 막대한 손실로 이어질 가능성을 충분히 내포하고 있다. 그러나 이러한 위협은 형태가 다양하고 불확실성이 높기 때문에, 기능적으로 단일 부처만으로는 효과적인 대응을 기대하기 어렵다. 예를 들어 해저 케이블 훼손과 같은 해저 시설의 경우, 과학기술정보통신부가 시설에 대한 정책을 수립하지만, 공익 또는 민간 사업자가 시설을 설치 및 관리한다. 그리고 이러한 시설이 해양에서 훼손될 때 사고 행위를 인지 및 단속하는 것은 해양경찰청이, 해양에서 발생할 수 있는 추가 위험 조사 및 해양 활동 규제는 해양수산부가, 행위자가 외국적 선박일 경우 행위자 처분에 관한 국제 공조 및 국외 정보 조사는 외교부가 담당하게 된다. 즉, 국가적인 해양 복합위협 발생 시 이를 적절하게 대응하기 위해서는 관련 부처의 업무

를 적절히 조정하고 보유 자원을 효율적으로 배치하며 유기적인 협력이 가능하도록 국가 차원의 위협 대응 지침 내지 전략이 구축되어야 한다.

구체적으로 이러한 국가전략은 국가적 해양 복합위협을 유형화하여 위협에 따라 관련 부처의 역할을 정의하고 책임기관과 협력 기관, 정보 공유기관을 구분하여 그 기능을 사전에 정의하여 위협을 효과적으로 예방 및 대응할 수 있도록 분야별 국가 기능을 정의해야 한다. 또한 국가전략은 이행 수단의 객관성, 자원의 효율적 배분, 위협의 효과적 억제를 위해 주요 국가에서 도입하여 적용하고 있는 위험성 평가 등 위협의 객관적 평가 기준을 포함해야 한다. 뿐만 아니라, 위협의 포괄적 대응을 위해, 정보를 다차원적으로 분석할 수 있는 기관별 필수 정보 체계를 구축할 수 있도록 해야 하며, 지역 및 국제 공조를 도모할 수 있도록 구성해야 한다.

특히, 정보의 분산은 광범위해지는 해양 복합위협을 기관마다 달리 분석하여, 국가 단위의 포괄적이며 효과적인 대응을 저해할 수 있다. 이는 본 연구 제2장 사례 분석에서 확인할 수 있듯이, 밀수(출)입 등 특정 위협에 관한 정보를 다양한 기관이 분절적으로 보유하고 있을 때, 단속의 누수가 발생하고 대응에 허점이 발생할 할 수 있다.[296] 이에, 미국, 영국 등 국외 선진국들은 관련 정보를 통합하여 분석하는 해양정보융합센터 내지 플랫폼을 구축하여 운영하고 있다.[297] 즉, 우리나라 또한 해양 복합위협에 대한 대응의 허점을 최소화하고 효과적인 통합 대응체계를 구축하기 위해서는 해양 복합위협 정보분석플랫폼을 구축하여 관계기관의 원천 정보를 융합·분석하여 결과를 공유하는 것이 필요하다. 다만, 효율적인 정보 관리를 위해 위협 발생 확인 및 단속을 위한 필수 정보는 정보분석플랫폼을 통해 정기적으로 공유하되, 분석된 정보 결과의 공유는 실질적인 대응 및 단속에

296) 본 보고서 제4장은 밀수(출)입과 관련된 범죄가 해양 국제범죄 중 가장 최우선적으로 대응해야 하는 해양 국제범죄 유형으로 분석하고 있다.
297) 본 보고서 제3장 참조

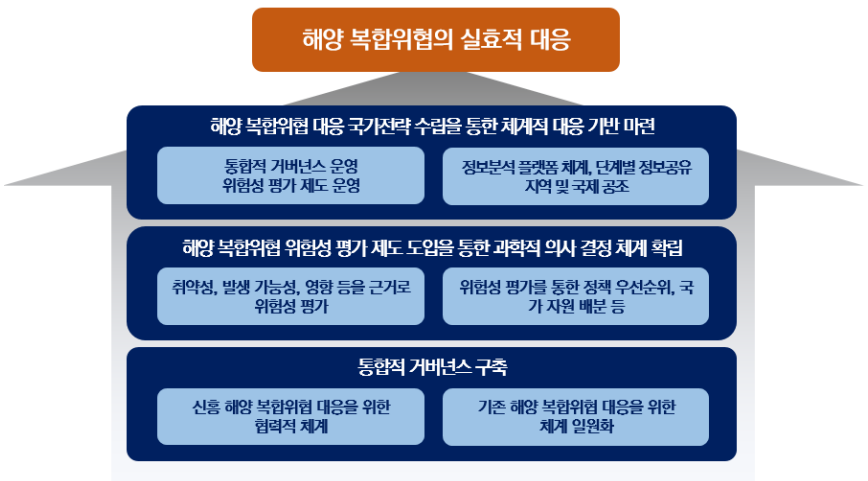
개입하는 기관으로 한정하는 단계적 정보 공유 체계가 구축되어야 할 것으로 판단된다. 즉 민감정보의 비인가 전파를 최소화하기 위해 위협 대응을 위한 필요 정보만을 관계기관에 공유하는 단계별 정부 공유 체계가 구축되어야 할 것으로 판단된다.

셋째, 통합적 대응체계와 해양 복합위협 대응 국가전략을 효과적으로 운영하기 위해서는 해양 복합위협에 대한 위험성 및 취약성을 체계적으로 평가하는 제도가 마련되어야 한다. 제2장에서 살펴본 바와 같이 최근 해양 복합위협은 전통·비전통 위협이 혼재하고, 효과는 광범위하지만, 행위자를 특정하기 어렵고, 그 수단 또한 다양하다. 이에, 모든 위협을 개별로 대응하기 위해서는 국가 자원을 소모적으로 배분 및 이용해야 한다. 다만, 국가 자원은 사실상 제한되어 있고 이를 합리적으로 배분 및 이용하기 위해서는 위협을 정량 및 객관화하여 위험의 우선순위에 따라 국가 대응 자원을 효율적으로 활용하는 것이 필요하다. 또한, 위협 대상의 취약성을 분석하여 이를 보완하기 위한 국가 자원 및 예산의 투입 우선순위를 정하는 것 또한 필요하다.[298] 제4장에서 언급한 바와 같이 미 USCG는 2005년부터 MSRAM을 제도적으로 도입하여 미 해안 전역에 대한 위험성 평가를 실시하고 있다. 이 평가 제도는 위협의 대상이 될 수 있는 주요 연안 시설 및 지역을 중심으로 위협 발생가능성, 취약성, 영향을 평가한다. 그리고 그 평가 결과를 통해 우선적으로 대응해야 하는 위협의 형태, 보호해야 하는 대상을 도출하고 이를 중심으로 국가전략을 개발하고 국가 자원을 배분한다. 이에, 우리나라 또한 한정된 자원으로 모든 위협에 대응하는 소모성 정책을 수립하기보다 해양 복합위협에 대한 객관적 평가 제도를 도입하여 보호대상 및 위협에 대한 정기적 평가를 실시하여 객관적 대응체계 및 자원 배

298) US Government Accountability Office(2011), pp. 37-38. 미 USCG는 이 자료를 통해 해양위협을 프로파일링하고, USCG 운영 계획과 자원을 객관적으로 분배하고, 지역별로 위협과 대상을 우선순위화 하여 효과적인 위협 대응이 가능하도록 USCG 위협 평가 체계인 MSRAM을 운용한다고 설명하고 있다.

분이 이루어질 수 있도록 해야 할 것이다. 즉, 제한된 국가 자원으로 해양 복합위협을 효과적으로 억제 및 대응하기 위해서는 위협 유형 및 대상의 위험성 내지 발생가능성을 평가하여 우선순위에 따른 대응체계를 수립하고, 개별 대상의 취약성을 중심으로 필수적인 장비 및 시스템을 구비해야 한다.

〈그림 5-2〉 해양 복합위협 실효적 대응 방안 방향



자료: 저자 작성

제2절 해양 복합위협의 효과적 대응을 위한 정책 방안

1. 해양 복합위협 통합 대응체계 구축

앞의 국외 사례에서도 확인한 바와 같이 주요 국가들의 해양 복합위협에 대한 대응체계는 일원화된 체계를 구축하거나 또는 현장 대응 기관 간 유

기적인 협력을 위해 통합 플랫폼을 구축하여 운영하고 있다. 미국의 경우 국토안보부를 중심으로, 일본은 해상보안청을 중심으로, 영국은 합동해양안보센터를 운영하여 해양 복합위협에 대한 일원화된 대응체계를 구축하고 있다. 이는 해양 복합위협의 관할 및 대상에 따라 다양한 대응 기관이 개입됨에도 불구하고 일원화된 부처 체계 내지 통합플랫폼을 통해 위협을 즉각적으로 대응하여 그 영향을 최소화하기 위함이다. 반면, 해양 복합위협에 대한 국내 대응체계는 앞에서도 살펴본 바와 같이 다양한 부처가 소관 법령에 따라 분절화되어 운영되고 있다. 특히, 우리나라의 해양 복합위협의 대응체계는 크게 공간적 관할과 사물 관할을 기준으로 구분되어 있다. 먼저 공간적 관할은 「국제선박항만보안법」에 따른 무역항을 중심으로 구축된 항만보안체계와 그 외 해안지역을 대상으로 해양경찰청을 중심으로 구축되어 있는 일반 치안 및 질서 유지 체계이다. 다음으로 사물 관할은 해양국제범죄, 해양테러, 해양 사이버위협 등 구체적인 대상에 따라 개별 기관에 분산되어 있는 사물 관할을 의미한다. 이에 본 절에서는 앞에서 분석된 개별 관할의 한계점을 중심으로 해양 복합위협 통합 대응체계 구축 방안에 대해 살펴본다.

1) 공간에 대한 통합 대응체계

해양 복합위협과 관련한 국내 대응체계는 공간적 관점에서 다음과 같이 한계가 존재한다. 첫째, 대다수 대응체계가 관할에 따라 기관 간 유기적인 협력체계보다, 법에서 정해진 권역에 따라 독립적으로 운영된다. 이는 해양에서 연안까지 연속적으로 발생하는 해양 복합위협을 분절적으로 대응할 수밖에 없는 결과로 연결되고 하나의 일련의 상황에 대해 대응 공백 내지 지연을 발생시킬 수 있다. 제2장과 제4장에서 분석한 바와 같이 밀입(출)국 등 우리나라 해역에서 가장 빈번히 발생하는 해양 복합위협은 공간을 넘어 연속적으로 위법한 행위가 이루어진다. 반면, 항만시설소유자 또는 국제항

해선박소유자는 항만 내 육상구역에서 수상구역으로 벗어난 밀항자에 대응할 수 있는 시설 내지 자원을 보유하고 있지 않다. 이에, 대부분 경우 경비함정을 보유하고 있는 해양경찰에게 상황을 전파하여 검거 내지 단속을 실시하고 최종적으로 밀입(출)국에 권한을 가진 출입국·외국인청에 범법자 내지 위법 행위자를 인계한다. 다만, 이러한 일련의 협업 중 관할의 사각지대 내지 책임소재가 불분명한 상황이 발생할 경우, 유관부처 간 책임 회피 경향이 있을 수 있으며, 이는 위협의 발생가능성을 내재화할 수 있다.[299]

특히, 우리나라는 공간적으로 「국제선박항만보안법」에 따른 무역항 등에 대한 위협 대응체계와 일반 연안의 위협에 대한 대응체계가 구분되어 있다. 무역항 등 항만의 경우, 주요 국가 시설로서 「국제선박항만보안법」에 따른 보안위원회 내지 「테러방지법」에 따른 항만 테러대책협의회를 통해 기관별 협업으로 대응이 이루어진다. 반면, 무역항 등을 제외한 일반 연안의 경우, 해양경찰청 함정 내지 육군 레이더 등을 통해 감시가 이루어지고 이상행동 발견 시 단속 권한이 있는 해양경찰청에서 주로 대응을 실시한다. 이에 앞에서 살펴본 바와 같이 항만-일반 연안-육상으로 하나의 위협이 연속적으로 이동할 때, 책임 및 권한의 전환, 관련 기관 간 지원이 불명확하며, 특히, 일반 연안의 경우, 위협의 행위가 해상에서 육상까지 연속된 경우, 출입국·외국인청, 관세청 등 소관 법령에 따른 관련 기관과의 협업이 이루어지고 있지만, 관련 근거가 미약하고 그 절차가 일관되지 않는다.

따라서 이러한 문제를 해결하기 위해서는 우선적으로 해양 복합위협을 공간적으로 통합 대응할 수 있는 대응체계가 갖추어져야 한다. 이를 위해 먼저 영역별로 각 기관의 책임 소재를 분석하면 먼저, 해양수산부는 31개 무역항 등에 「국제선박항만보안법」에 따른 항만시설의 보안사고에 최종 책임을 지며, 항만공사, 항만보안공사, 지방해양수산청은 실무책임을 진다.

299) 함혜현·전봉조·이장욱, 앞의 책, p. 380.

다만, 해양경찰청은 항만구역의 수상구역에서 단속 및 검거를 실시한다. 출입국·외국인청의 경우, 항만을 포함한 연안터미널에서의 출입국 사무에 관한 단속 및 검거에 책임을 지고, 관세청은 밀수 혐의 선박 검색 등 밀수 방지에 관한 책임을 진다.

〈표 5-1〉 해양 복합위협 공간별 책임 분산 구조

구분		해양 수산부	항만공사 (보안공사등)	해양 경찰청	출입국·외국인청	관세청	군
구분	영역						
무역항 등 항만 시설	육상	A/R	R	C	A/R (밀입(출)국 등)	A (밀수 등)	N/A
	수상	A	R	A/R	C	A/R (밀수 등)	N/A
연안	육상	I	N/A	C	A/R (밀입(출)국 등)	A/R (밀수 등)	C
	수상	I	N/A	A/R	C	A/R (밀수 등)	C

주: A(Accountable) – 최종 책임자, C(Consulted) – 협력 기관, I(Informed) – 통보 기관, R(Responsible) – 실행 책임자
자료: 국제선박항만보안법, 해양경비법, 출입국관리법, 관세법 등을 참조하여 저자 작성

이러한 분석을 근거로 해양 복합위협이 해양에서 발생하거나 해양과 연계하여 발생하는 복합위협임을 고려할 때, 해양 법집행기관을 중심으로 일원화된 체계를 구축하는 것이 가장 효율적일 것으로 판단된다. 특히, 해양경찰청의 경우, 무역항 등 항만시설과 연안의 수상구역에서 단속 및 검거를 책임지고 있으며, 그 외 지역에서는 단속 및 검거를 위한 주요 협력 기관으로 폭넓은 관할을 가지고 있다. 뿐만 아니라, 관세청은 밀수 의심 선박의 해상검색을 포함하여 육상 및 수상에서 일어나는 밀수와 관련된 모든 업무에 대해 책임을 지고 있으므로 이러한 법집행 자원과 권한을 가진 기관을 중심으로 통합 대응체계를 구축하는 것이 효율적일 것으로 판단된다.

2) 사물 관할에 대한 통합 대응체계

해양의 복합위협이 점차 다변화되고 있어 위협 대상 또는 활동에 따라 개별적으로 대응하고 있는 현재의 대응체계를 일원화하여 통합적으로 운영하는 대응체계가 필요하다. 이는 해양 복합위협에 대한 분절적 대응과 관할의 사각화를 최소화하고 위협의 효과적 대응을 위한 자원의 효율적인 운영을 가능하게 한다. 특히, 해양 복합위협에 대한 기관의 책임과 권한을 명확히 하여 민감하거나 복잡한 사건에 대해 유관부서의 협업 또는 책임 회피를 제거하고 책임 있는 대응을 유도한다. 다만, 현재 국내에는 해양 복합위협과 관련하여 이미 다양한 협의체가 구성 및 운영되고 있다. 이에, 장기적으로 해양 복합위협 통합 대응체계가 위협 대상별 책임 및 권한에 있어 이들 협의체와의 관계 정립이 제도적으로 이루어져야 한다. 특히, 해양 복합위협 위험성 평가를 통해 위협에 대응하기 위한 가장 효과적인 체계를 도출하고, 관련 협의체의 권한 및 책임을 조정하여 최종 책임 및 조정 기관을 규정하는 것이 필요할 것으로 사료된다.

이를 위해 현재 해양 복합위협 대상별 책임 분산 구조를 분석하면 다음과 같다. 해양 국제범죄의 경우, 「국제선박항만보안법」에 따른 보안사고가 무역항 등 항만시설에서 발생했을 경우, 항만공사 등 항만시설소유자가 현장 책임자로서 사건에 대응하며, 해양수산부가 보안위원회 등을 통해 정책결정자로서 최종 권한과 책임을 가진다. 그 외 연안 지역에서 발생하는 국제범죄의 경우, 군에서 감시 자원을 통해 해상에서의 이상행동 인지를 지원하며, 해양경찰청이 경비·치안 관리 기관으로 해양 국제범죄에 대한 권한 및 책임을 가진다. 다만, 밀입(출)국, 밀수(출)입의 경우, 「출입국관리법」, 「관세법」 등에 따라 법무부 출입국·외국인청과 관세청이 관할 업무로 최종 권한과 책임을 가진다. 해적의 경우, 「해적피해예방법」에 따라 최종 권한과 책임을 해양수산부에서 가지며, 관련 정보 및 훈련, 현장 대응은 군과

외교부에서 담당한다. 해양테러의 경우, 무역항에서의 드론 운용 등에 관한 사항은 「국제선박항만보안법」에 따라 규율을 받게 되어 해양수산부가 최종 책임과 권한을 가지며, 불법무기 밀수 등에 관해서는 「관세법」에 따라 관세청이 최종 권한을 가진다. 그 외 일반적인 해양테러에 관한 정책 수립 및 대응에 관한 사항은 해양경찰청이 「테러방지법」에 따라 권한과 책임을 가진다. 마지막으로 해양 사이버위협의 경우, 안전과 범죄로 구분하여 해양수산부와 해양경찰청이 각각 대상에 따라 권한과 책임을 가진다.

〈표 5-2〉 관련기관 해양 복합위협 대상별 책임 분산 구조

해양 복합위협 분류			해양수산부	항만공사(보안공사등)	해양경찰청	출입국·외국인청	관세청	군
해양국제범죄	밀입(출)국	무역항	R	R	C	A/R	–	–
		연안	I	–	C/R	A/R	–	C
	밀수(출)입	무역항	R	R	C	–	A/R	–
		연안	I	–	C/R	–	A/R	C
	납치		I	–	A/R	C	–	C
	해적 및 무장강도		A/R	–	A/R	–	–	C/R
해양테러	해양테러		C	C	A/R	–	–	C
	드론공격	무역항	A/R	R	C	–	–	C
		연안	I	–	A/R	–	–	C
	해저시설 공격		C	–	A/R	–	–	C/R
	대량살상무기	무역항	A/R	R	R	–	A/R* 밀수	C/R
		연안	–	–	A/R	–	A/R* 밀수	C/R
해양사이버위협	사이버공격	안전	A/R	R	I	–	–	–
		범죄	I	R	A/R	–	–	–
기타	기타		A/R	R/I	A/R	–	–	–

주: A(Accountable) – 최종 책임자, C(Consulted) – 협력 기관, I(Informed) – 통보 기관,
R(Responsible) – 실행 책임자
자료: 국제선박항만보안법, 해양경비법, 출입국관리법, 관세법 등을 참조하여 저자 작성

기관별 권한과 책임 분산에 더해 해양 복합위협과 관련하여 운영되고 있는 위원회의 책임과 권한을 살펴보면 다음과 같다. 마약의 경우, 마약류대책협의회가 「마약류관리법」에 따라 국무총리실 산하에 설치되어 있으며, 식품의약품안전처를 중심으로 운영되고 있다.[300] 마약류대책협의회의 임무 중 마약 밀수 단속에 관한 전체적인 사항은 관세청이 담당하며, 그 외 요트 등 해상에서의 마약 투약, 입출항 선박의 불법 마약 소지 등 해양 마약류 사범 단속에 관한 사항은 해양경찰청이 담당한다. 또한 국내 대테러 기능을 위해 국가테러대책위원회가 「테러방지법」에 따라 국무총리를 위원장으로 설립되어 있으며, 관계기관 협의체인 대테러센터가 간사기관으로서 실무운영을 위해 국무총리실 산하에 설치되어 있다.[301] 국가테러대책위원회는 테러가 발생하거나 발생할 우려가 현저한 경우, 분야에 따라 테러사건대책본부를 설치 및 운영해야 하며, 해양테러의 경우 해양경찰청이 사건대책본부를 설치하고 운영해야 한다.[302] 국가사이버안보 및 위협과 관련해서는 「사이버안보 업무규정」에 따라 국가정보원 산하에 국가사이버안보센터를 설치 및 운영하고 있다.[303] 국가사이버안보센터는 2024년 “국가 사이버안보 기본계획”을 발표하고 부처별로 추진해야 할 과제를 설정하고 있으며, 그중 해양수산부는 관계부처로 해사·항만분야 사이버보안을 강화하는 업무를 담당한다.[304]

300) 마약류관리법 제4조의2
301) 테러방지법 제5조, 제6조
302) 테러방지법 시행령 제14조
303) 사이버안보 업무규정 제4조
304) 국가사이버안보센터(2024.9.2.)(검색일: 2025.9.13.)

〈표 5-3〉 협의체별 해양 복합위협 대상별 책임 분산 구조

해양 복합위협 분류		마약류대책협의회 (식품의약품안전처)	국가테러대책위원회 (대테러센터)	국가사이버안보 (국가사이버안보센터)
해양 국제범죄	밀입(출)국	-	-	-
	밀수(출)입	A/R	-	-
	납치	-	A/R	-
	해적 및 무장강도	-	A/R	-
해양테러	해양테러	-	A/R	-
	드론 공격	-	A/R	-
	해저시설 공격	-	A/R	-
	대량살상무기	-	A/R	-
해양 사이버위협	사이버 공격	-	-	A/R
기타	기타	-	A/R	-

주: A(Accountable) – 최종 책임자, R(Responsible) – 실행 책임자
자료: 마약류관리법, 테러방지법, 사이버안보업무규정 등을 참조하여 저자 작성

국내 해양 복합위협과 관련하여 이미 설치되어 있거나 기능을 하고 있는 협의체는 국무총리실 산하 내지 국무총리실을 위원장으로 운영되고 있다. 다만, 국가안보실의 국가정보원 국가사이버안보센터의 경우, 개별법에 분산되어 있는 권한을 정부 합동 '국가 사이버안보 기본계획'을 중심으로 각 부처가 국가 계획에 부합하여 운영할 수 있도록 플랫폼 역할을 담당하고 있다. 이는 사실상 사이버라는 분야가 모든 영역에서 다양하게 관리 및 운영되고 있는 반면, 관련 위협은 다차원 및 다영역에서 연속적으로 발생할 수 있기 때문에, 개별 기관의 권한 및 책임에 따라 민관합동 통합대응체계를 구축 및 운영하기 위하여 전담조직을 구축한 것이다.[305] 해양 복합위협의 경향도 현재 다영역에서 복합적으로 발생하는 경향이 짙어지고 있다. 사이버를 수단으로 물리적 공격이 병합되거나, 국가 행위자가 군사적 또는 공적 수단을 동원하여 타국에서 위법한 행위를 벌이는 등의 전통 및 비전

305) 사이버안보 업무규정 제4조, 제5조 등 참조

통 위협이 복합적으로 발생하고 있다. 이에, 해양 복합위협은 필연적으로 다양한 기관이 권한과 기능에 따라 개입되어야 하므로 현재의 권한과 책임을 최대한 유지하면서, 각 기능을 효과적으로 운영할 수 있는 통합적 협력 체계가 구축되어야 한다.

3) 해양 복합위협 통합 대응체계 구축 방안

앞에서 살펴본 바와 같이 현재 해양 복합위협 대응을 위한 권한과 책임은 분산되어 있는 동시에 주요 위협에 대해서는 권한과 책임이 중첩되어 나타나고 있다. 반면, 분산된 권한과 기능을 통합하고 책임에 따라 업무를 조정하는 국가테러대책위원회와 같은 중앙협의체가 존재하지 않아 업무의 효율성이 떨어지며, 책임 회피 등으로 인한 대응 공백까지 나타날 수 있다. 이에, 이러한 권한의 중첩과 비효율성을 해소하고 효과적인 위협 대응을 위해서는 이를 통합적으로 관리하기 위한 중앙협의체('국가해양위협대책위원회'(가칭))가 설치 및 운영되어야 할 것으로 판단된다.

(1) 통합 대응체계 기능

먼저, 국가해양위협대책위원회는 해양 복합위협에 관한 국가의 정책을 수립하고 평가하도록 권한이 부여되어야 한다. 이는 장기적으로 위원회가 '국가 해양위협 대응 기본계획' 등과 같은 중장기 대책을 수립하여 기술 발전 및 위협 양태 변화에 따라 유관기관의 기능을 적절히 조정 및 수정할 수 있도록 정책적으로 지원하기 위함이다.

다음으로 국가해양위협대책위원회는 해양 복합위협과 관련된 상황 발생 시 이에 대한 관계기관의 역할을 분담 및 조정할 수 있는 권한이 부여되어야 한다. 국가해양위협대책위원회는 공간 및 대상에 따라 분산 및 산재되

어 있는 유관기관 기능과 역할을 조정하고, 해양 복합위협 유형에 따른 대응 방안을 최종적으로 결정하는 권한과 책임을 담당해야 한다. 특히, 관할의 중첩으로 책임 회피 내지 대응 사각지대가 발생할 수 있는 영역을 확인하여 해양 복합위협 대응체계 공백을 최소화해야 한다. 이를 위해, 국가해양위협대책위원회는 해양 복합위협 위험성 평가 등에 관한 제도를 수립하여 운영할 수 있으며, 위협에 따른 관련 기관의 협력체계를 지시하는 지침을 개발하여 적용할 수 있다.

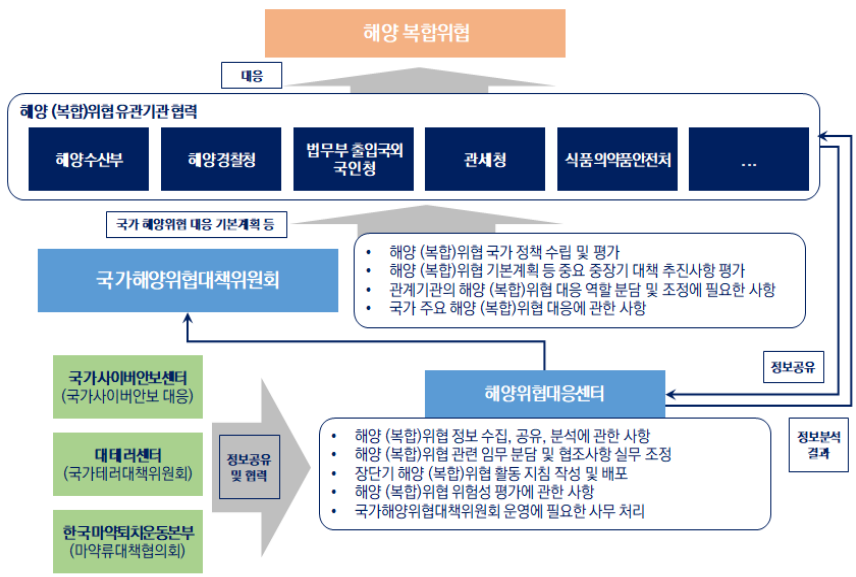
또한 국가해양위협대책위원회에는 상황 발생 시 필요에 따라 관련 기관의 자원을 즉각적으로 재배치 내지 활용할 수 있는 권한 또한 주어져야 할 것으로 판단된다. 즉, 국가적 위협에 대해 위원회가 직접 대응할 수 있는 권한을 가지도록 하여, 다양한 기관이 개입하게 되는 국가적 위기 상황에서 대응 기관들이 유기적으로 협력할 수 있는 일원화된 체계를 구축해야 한다. 이는 대형 해양 복합위협 발생 시 대응의 사각지대를 미연에 해소하고 적절한 대응이 이루어질 수 있도록 제도적 근거를 제공한다.

마지막으로 국가해양위협대책위원회의 효율적 운영을 위해서는 위원회 예하 실무 운영을 위한 해양위협대응센터(가칭)가 설치되어야 한다. 「테러방지법」상 국가테러대책위원회는 대테러센터를 예하에 설치하여 국가테러대책위원회의 실무를 조정하고 관련 기관에 국가대테활동에 관한 지침을 제공한다.[306] 마약류대책협의회 또한 「마약류관리법」에 따라 실무를 위한 분과위원회와 실무협의회를 설치하여 최상위 협의체의 업무를 지원한다.[307] 이에 국가해양위협대책위원회 예하에 관련 기관의 실무 조정 및 위원회 사무 처리를 위한 해양위협대응센터가 설치되어야 할 것으로 판단된다. 다만, 해양위협대응센터는 위원회의 사무 처리에 더해, 국가 해양 복합위협에 대한 위원회의 대응 업무를 지원하기 위해 유관기관별로 산재되어

306) 테러방지법 제6조
307) 마약류관리법 제2조의4

있는 위협 관련 정보를 수집, 분석, 공유할 수 있는 기능을 갖추고 이를 정보플랫폼을 통해 운용될 수 있도록 체계가 구축되어야 한다. 또한 해양위협대응센터는 위원회의 관련 정책 수립과 결정을 지원하기 위해 해양 복합위협 위험성 평가 제도를 운영하는 기능 또한 갖추어져야 할 것으로 판단된다. 이는 다양한 기관의 해양 복합위협 대응 업무를 사전에 조율하여, 위원회의 효율적 의사결정을 지원하고. 정보분석 및 위험성 평가를 통해 광범위하고 다양한 해양 복합위협을 객관적이고 합리적으로 대응할 수 있도록 지원하기 위함이다.

〈그림 5-3〉 국가해양위협대책위원회(가칭) 운영 체계



자료: 저자 작성

(2) 통합 대응체계 구축 로드맵

국가해양위협대책위원회의 구축은 광범위한 대상과 다양한 기관의 업무 연관성을 고려하여 단계별로 추진해야 한다. 먼저, 단기적으로 해양 복합위

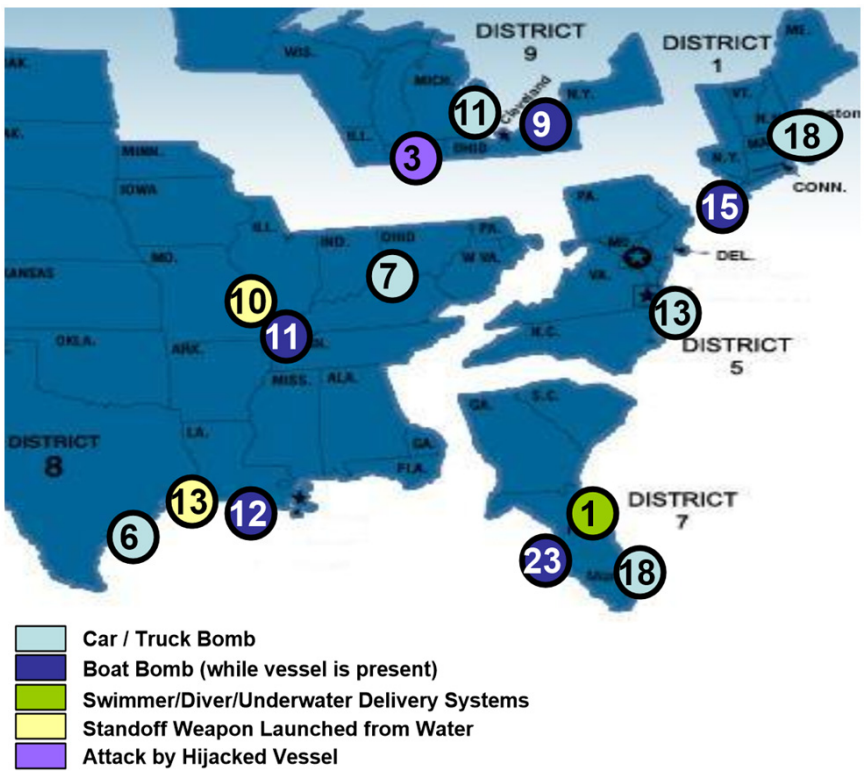
협에 관한 관련 기관들의 권한과 책임을 조정하는 해양위협대응센터(가칭)의 설립을 추진해야 한다. 이는 기관별로 소관 법령에 따라 주어진 권한과 책임을 실무 차원에서 조정하는 역할을 담당한다. 또한 해양위협대응센터는 개별 기관에 산재되어 있는 해양 복합위협에 대한 감시 및 단속에 관한 정보를 수집, 융합, 분석, 공유할 수 있는 기능을 갖추어야 한다. 이는 앞에서도 언급한 바와 같이 국가해양위협대책위원회의 합리적인 업무 조정 기능을 실현하기 위해 객관적인 데이터를 확보하기 위함이다. 다만, 위원회의 설립은 장기적으로 추진되어야 하는바, 단기적으로 정보의 수집, 분석을 위한 제도적 틀을 갖추고 향후 정보분석플랫폼 구축을 통해 관련 정보를 데이터화하는 것이 필요할 것으로 판단된다.

해양위협대응센터의 설립 및 운영과 더불어, 위원회 책임과 권한의 범위를 확인하기 위해 단기적으로 해양 복합위협 대응에 관한 법령 분석이 필요하다. 이는 개별 부처에 분절적으로 산재되어 있는 권한 및 책임의 범위를 확인하고 이를 통해 향후 설립될 국가해양위협대책위원회의 역할 범위를 설정하는 근거가 된다. 또한, 이러한 법령 분석은 향후 해양 복합위협 대응 기관으로서 위원회에 참여하는 기관의 범위와 개별 기관의 참여 범위를 정하는 기준이 된다. 마지막으로 법령 분석은 해양 복합위협에 대응하기 위한 현행 체계와 최근 위협 경향 사이의 제도 격차를 분석하여 이를 정책적으로 대응할 수 있는 방안을 수립할 수 있도록 근거를 제공한다.

국가해양위협대책위원회 설립을 위한 중기 방안으로는 해양 복합위협 대상 및 주요 해안시설, 권역별 연안에 대한 위험성 평가가 이루어져야 한다. 이를 위해서는 미 USCG의 MSRAM 등 국외 선진국들이 이미 활용하고 있는 해양 복합위협 내지 위협 위험성 평가 제도를 수정하여 국내에 적절히 도입할 필요가 있다. 예를 들어, USCG의 경우, 해양 복합위협의 위험성 평가를 위해 MSRAM을 개발하여 적용하고 있다. MSRAM은 위험성 평가를 위해 위협 발생가능성, 영향, 취약성 등을 최대한 정량화한 자료를 근거

로 위험성을 도출한다. 특히 정량적 자료에는 인구사회학적 통계, 피해 규모(1차 및 2차), 사상자수, 환경 피해, 보안시스템(민간/USCG 등), 대응력(보안 시설 수준, 시스템 및 장비 등), 발생 가능한 위협의 정도 등 다양하고 광범위한 자료가 포함된다. USCG는 MSRAM을 통한 위험성 결과를 해양 복합위협 대응을 위한 지역별, 권역별, 국가적 전략을 수립에 활용하고 관계기관에 공유하여 국가 자원의 배분 등에도 활용한다.[308]

〈그림 5-4〉 USCG MSRAM 위험성 평가 결과 예시



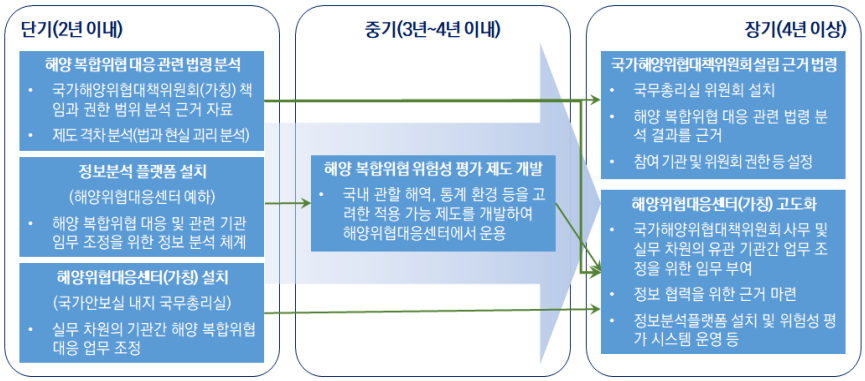
자료: Brady Downs, LCDR(2008) 참조하여 저자 편집

308) Downs(2008); US Government Accountability Office(2011), pp. 37-38.

반면, 우리나라의 경우, 해양위협에 대한 위험성 평가를 제도적으로 운영하고 있지 않다. 이에, MSRAM과 같이 객관적인 위험성 평가를 위한 분야별 자료를 정량화 또는 통계로 관리하고 있지 않다. 이에, 단기적으로 우리나라 관할 해역의 해양 복합위협을 평가하기 위한 위험성 평가 제도를 개발하는 것이 필요하며, 중기적으로 위험성 평가를 위해 필요한 통계를 전산화하여 지속적으로 수집 및 관리하는 체계가 마련되어야 할 것으로 판단된다.

장기적으로 국가해양위협대책위원회(가칭)를 설립하기 위한 개별 법령의 제정과 해양위협대응센터 고도화를 통한 효과적인 해양 복합위협의 통합적 대응체계가 마련되어야 한다. 국가해양위협대책위원회의 주요 기능을 해양(복합)위협에 대한 국가 정책 수립 및 평가, 관련 기본계획 등 중요 중장기 대책 추진사항 평가, 관계기관의 역할 분담 및 조정, 국가 주요 해양 (복합) 위협의 대응에 관한 사항 등으로 정하고 이를 국무총리실 위원회로 정하는 근거 법령 제정을 장기적으로 추진해야 한다. 특히, 위원회의 권한과 책임, 적용 범위를 명확히 하기 위해 해양 복합위협 대응 관련 법령 분석의 결과를 활용해야 한다. 또한 설립되는 국가해양위협대책위원회(가칭)의 임무를 보좌하고, 해양 복합위협의 위험성 평가를 실시하고 실무적으로 해양 복합위협에 관한 임무 분담 및 협력을 추진하고, 관련 임무에 대한 기관별 지침을 작성하며, 해양 복합위협에 관한 정보분석플랫폼을 운영하기 위해 국가해양위협대책위원회(가칭)의 설립 법령에 해양위협대응센터의 기능을 명시하는 방안이 추진되어야 한다.

〈그림 5-5〉 국가해양위협대책위원회(가칭) 구축 로드맵



자료: 저자 작성

(3) 통합 대응체계 구축을 위한 제도 개선 방안

장기적으로 「해양 복합위협 관리법」(가칭) 내지 「해양 복합위협 대응 업무규정」(가칭) 필요할 것으로 판단된다. 다만, 단기적으로 해양위협대응센터 설치 및 운영을 위한 지침의 제정이 필요할 것으로 판단되며, 이 지침은 「테러방지법」 내지 「국가정보원법」, 또는 「해양경비법」의 하위 규정으로 제정하여 운영할 수 있을 것으로 판단된다. 이는 해양 복합위협에 관한 위험성 평가 제도를 중기에 걸쳐 개발하고 국가해양위협대책위원회의 권한 및 역할과 관련 기관의 협력 범위를 장기에 걸쳐 분석 및 도출한 이후 하나의 제도로 제정하기 위한 단기적 방안이 될 수 있다. 특히, 해양위협대응센터의 설치가 향후 국가해양위협대책위원회 설립 및 관련 제도 구축을 위한 것임을 고려할 때, 해양위협대응센터 설치 및 운영에 관한 지침은 유관기관의 업무를 효율적으로 조정할 수 있고 향후 위협에 관한 정보를 주도적으로 확보하고 활용할 수 있는 기능을 중심으로 제정되어야 할 것으로 판단된다.

장기적 제도로서 「해양 복합위협 관리법」 내지 「해양 복합위협 대응 업무규정」은 국가해양위협대책위원회 설치 및 운영, 해양 복합위협의 유형, 해양위협대응센터 운용, 위험성 평가, 기관 간 협력체계 구축 등을 주요 내용으로 구성할 수 있을 것으로 판단된다. 유사입법례로 「통합방위법」, 「테러방지법」, 「사이버안보 업무규정」이 있으며, 이들 규정의 주요 내용은 적용의 대상, 협의체 구성 및 운용, 기관 간 협력체계 구성, 관련 제도 운용을 위한 규정들로 구성되어 있다. 다만, 「사이버안보 업무규정」은 「국가정보원법」에 따른 대통령령으로서 제정되어 있어 「통합방위법」 또는 「테러방지법」과 법적 지위를 달리하고 있다. 그러나 법률이 아닌 대통령령은 법률보다 개정이 용이하여 사이버 기술의 급속한 변화에 효율적으로 대응할 수 있다는 장점이 있다고 할 수 있다. 해양 복합위협 또한 실현 수단이 사이버와 빈번히 연계되고, 해양 사이버위협을 해양 복합위협의 한 유형으로 구분할 수 있어 이러한 특성을 반영한 제도의 수립이 이루어져야 할 것으로 판단된다.

〈표 5-4〉 「해양 (복합)위협 관리법」(가칭) 주요 내용

해양 (복합)위협 관리법	테러방지법	통합방위법
• 제1장 총칙 • 제2장 국가해양위협대책위원회 • 제3장 해양위협대응센터 • 제4장 기관 간 협력체계 구축 등 • 제5장 해양위협 위험성 평가 • 제6장 해양위협 정보플랫폼 • 제7장 교육 및 훈련 • 제8장 보칙 • 제9장 벌칙	• 제5조 국가테러대책위원회 • 제6조 대테러센터 • 제8조 전담조직의 설치 • 제9조 테러위험인물에 대한 정보 수집 등 • 제10조 테러예방을 위한 안전관리대책의 수립	• 제1장 총칙 • 제2장 통합방위기구 운용 • 제3장 경계태세 및 통합방위사태 • 제4장 통합방위작전 및 훈련 • 제5장 국가중요시설 및 취약지역 관리 • 제6장 보칙 • 제7장 벌칙

자료: 테러방지법, 통합방위법, 사이버안보 업무규정 등을 참조하여 저자 작성

2. 해양 복합위협 대응 국가전략 수립

1) 필요성

통합적 거버넌스의 효과적 운영을 위해서는 모든 대응 활동의 지침이 되는 최상위 계획인 국가전략이 필요하다. 특히, 해양 복합위협 대응을 위한 국가전략은 불확실하고 복잡한 국내외 환경 속에서 다양한 국가 자원을 통합적으로 활용하여 국가의 목표를 효율적으로 달성하고 국익을 보호하기 위해 요구된다. 최근 해양에서 발생하는 위협은 밀입국, 마약 밀수, 인신매매 등 조직적 범죄부터 해저케이블 훼손, 해적 및 무장강도, 주요 해양시설 공격, 기타 해양테러 위협 등 국가 안보에 영향을 미치는 행위로 다양하게 발생하고 있다. 그리고 이러한 행위들은 최근 사이버 수단과 연계하여 추적이 어렵고 발생을 예측하기 어렵게 한다. 반면, 이러한 행위들의 영향은 과거와 달리 지속적이고 광범위하며, 사회적으로 많은 피해를 미치기도 한다. 그러나 위협에 대한 부처별 단편 대응은 초기 억제와 피해 최소화에 한계를 가지고, 따라서 위협 대응에 대한 다양한 정부기관의 협력을 요구한다. 결국, 최근 불확실성이 가중되고 있는 해양안보 환경은 해양 복합위협에 효과적으로 대응하고 국익을 보호하기 위해 제한된 국가 자원을 효율적으로 활용하는 통합적 국가전략을 요구한다.

이러한 국가전략은 해양 복합위협으로부터 국가 핵심이익을 보호하기 위한 비전과 목표를 제시하고, 이를 달성하기 위해 국가 자원을 활용하기 위한 방안 그리고 관계기관의 효과적인 협력체계를 규정해야 한다. 이를 위해 해양 복합위협 대응을 위한 국가전략의 목표는 항만·연안·원해·사이버에 걸친 다차원적 위협을 예방–대비–대응–복구 전 주기로 관리하고, 국제규범과 국내 법체계를 정합화하고 위험 기반으로 자원을 배분하여 효과적인 위협 대응을 실현하고 피해로부터의 회복탄력성을 갖추도록 설정되어야 한다. 글로벌 공급망과 원자재·식량·에너지 수입 의존도가 높은 우리 경제

구조상, 항만·해저케이블·LNG 기지 등 핵심 거점의 운영 중단은 곧 국가 경제 전반의 마비로 이어질 수 있다. 따라서 위험성·취약성 평가에 기반해 고위험 자산과 주요 해양시설에 국가 대비 자원을 우선 배분하고, 다양한 기관의 권한 및 책임을 실효적으로 운영하기 위한 상위 정책 방향이 필요하다. 결국, 해양 복합위협 국가전략은 예산·인력·기술을 위험 기반으로 배분해 효율성과 효과성을 높이고, 기관 간 역할 관계를 명확히 정립하여 책임성과 투명성을 담보하는 해양안보 거버넌스의 지침을 의미한다.

2) 주요 내용

해양 복합위협 대응을 위한 국가전략은 다음과 같이 다섯 가지 주요 내용으로 구성할 수 있다. 먼저, 국가전략은 최상위 계획으로서 국가 핵심이익을 구체적인 위협으로부터 보호하기 위한 국가기관의 유기적인 협력과 기능실현을 위해 수립되어야 한다. 따라서 해양 복합위협 대응 국가전략의 실질적인 이행력을 확보하기 위해서는 대응하고자 하는 대상의 정의와 범위가 구체적으로 제시되어야 한다. 이를 위해서 본 연구 2장에서 수행한 해양 복합위협의 유형 및 사례를 참고할 수 있을 것으로 판단된다.

둘째, 통합적 거버넌스이다. 국무총리실에 상설 위원회인 국가해양위협대책위원회를 설치하여, 해양 복합위협에 대응하기 위한 기본 계획 등 국가 정책을 수립하고 관련 기관의 권한과 책임을 상황에 따라 적시에 조정할 수 있도록 대응체계를 수립해야 한다. 특히, 해양 복합위협은 해양수산부, 해양경찰청, 군, 관세청, 출입국·외국인청, 경찰청, 국가정보원, 항만공사, 항만보안공사, 지자체 등 민·관·군·경이 함께 대응해야 하는 위협이다. 따라서 국가전략은 다양한 기관이 유기적인 협력을 통해 효과적인 대응을 실현할 수 있도록 구체적인 대응체계를 제시해야 한다.

셋째, 위험성 평가의 제도화다. 주요 해양시설 등 위협 대상, 공격 수단,

취약 지역 등에 대한 해양 복합위협의 위험성을 평가하여 국가 자원을 우선적으로 배정해야 하는 우선순위를 도출한다. 이는 공격 수단을 중심으로 위협 대상의 취약점을 분석하여 위협에 대응하기 위한 대상별 최적화된 정책을 수립할 수 있는 근거를 제공할 수 있다. 즉, 위협 대상 및 지역의 취약성을 근거로 필요한 국가 자원을 우선 배분하고 향후 갖추어야 하는 인력, 제도, 장비, 예산에 관한 정책 수립에 객관적 근거로 위험성 평가 제도를 활용할 수 있도록 국가전략 목표를 제시해야 한다.

넷째, 정보분석플랫폼의 구축 및 설치이다. 해양은 광범위한 공간적 범위로 인해 전체 해역에 대한 상시적인 감시체계를 구축하는 것이 불가능하다. 이에 해양의 활동을 탐지 및 감시하는 기관별 다양한 감시체계의 정보를 필요에 따라 싱글윈도를 통해 분석 및 공유하는 것이 필요하다. 즉, 해양수산부의 해적 및 해양안전정보, 해양경찰의 해양상황인식체계(MDA), 해군의 해양영역인식(MDA), 관세청의 관세정보시스템, 외교부의 제재정보 등 각 기관에 산재되어 있는 정보를 융합분석하는 정보분석플랫폼을 구축하여 해양 복합위협의 포괄적 예측 및 대응을 지원하도록 전략 목표를 제시해야 한다.

다섯째, 지역·국제 공조의 제도화이다. 항만공사·선사·통신·에너지 사업자와 정보 공유·훈련을 정례화하고, EU 및 ASEAN 등 지역 협력체의 사례를 참조해 공동 순찰 및 감시·정보교환·핵심해양인프라(해저케이블·파이프라인·풍력)의 보호를 위한 공조 체계를 구축해야 한다. UN은 매년 해양 및 해양법 결의서를 통해 해양위협의 탐지, 예방 및 억제를 위해 국가 간 정보 공유 강화, 협력을 통한 지속적인 역량 강화, 글로벌, 지역, 양자 차원에서의 국제협력이 필수적임을 강조하고 있다.[309] 따라서 해양 복합위협의 효과적 대응을 위해 해양의 국제성을 고려한 지역 및 국제 공조를 제도화하고 이러

309) United Nations General Assembly, op. cit., p. 21.

한 협력체 운영을 위한 센터를 설립할 수 있도록 전략을 수립해야 한다.

〈그림 5-6〉 해양 복합위협 대응 국가전략 개념도



자료: 저자 작성

3) 국가전략 수립 및 이행 로드맵

해양안보 국가전략은 해양의 지속적이고 평화적인 이용을 위해 최근 증가하고 있는 해양 복합위협에 효과적으로 대응하기 위한 최상위 국가전략 중 하나이다. 따라서 이러한 전략을 수립하기 위해서는 먼저, 해양 복합위협을 상시적으로 관리하는 범부처 또는 상위 기구가 존재해야 한다. 특히, 현재 국내에는 해양 복합위협을 다부처 협력체계를 통해 관할별로 대응하고 있으므로 이를 조정 및 통합할 수 있는 상설 기구를 개별 부처의 기능과 역할을 조정할 수 있는 국무총리실 내지 대통령실에 설치하는 것이 필요하다. 이러한 조직의 설치에 관한 로드맵 및 관련 제도는 앞의 해양 복합위협

통합 대응체계 구축을 참조할 수 있다.

설치된 상설 기구는 해양 복합위협의 예방 및 대응 활동과 관련된 제도 및 법령 분석을 실시하고 해양 복합위협 유형에 따른 기관별 협력체계의 한계와 사각지대를 확인해야 한다. 이후 이를 개선하기 위한 구체적 방안을 국가전략의 중점 추진 분야로 설정하고 이를 이행하기 위한 간사 기관 내지 관리 기관을 선정하는 것이 필요하다. 다만, 이러한 간사 또는 관리 기관은 국가전략의 효과적 이행을 위해 해양 법집행기관 또는 위협을 가장 주도적으로 대응하는 부처로 선정하는 것이 바람직할 것으로 판단된다. 호주의 경우, 우리나라와 유사하게 다부처 협력체계를 통해 해양위협에 대응하고 있으며, 이러한 대응체계의 효율적 운용을 위해 국가전략과 범부처 지침을 작성하여 적용하고 있다.[310] 또한 호주는 범부처 전략과 지침의 효과적 운영을 위해 호주국경수비대(Australian Border Force)에 정보융합 및 분석플랫폼을 설치하고 개별 기관의 기능 및 임무를 조정하여 위협의 효과적인 감시 및 대응이 이루어지도록 유도하고 있다.

3. 해양 복합위협 위험성 평가 제도 도입

1) 위험성 평가 활용 사례 및 효과

해양 복합위협에 관한 국외 위험성 평가 제도는 앞에서 언급한 바와 같이 미국 USCG MSRAM이 대표적이다. 그러나 미국 외에도 호주, 영국 등도 전통·비전통 해양위협을 평가하기 위한 국가 체계를 구축하고 있다. 특히 영국의 경우, 국가해양안보전략을 통해 정기적으로 해양위협에 관한 위험을 평가하도록 정하고 있다.[311] 영국의 국가해양안보전략에 따른 해양위험

310) Australian Government(2021, pp. 2-10; 2020, pp. 1-13.)
311) 현재의 영국 국가해양안보전략은 2014년에 이어 두 번째로 수립된 전략으로 2022년 8월부터 2027년

성평가(Maritime Risk Assessment)는 주요 위험에 대응하기 위한 범부처에 걸친 포괄적 평가로 주요 해양 이해관계를 식별·평가·대응하는 국가 차원의 위험성 평가 체계이다. 해양위험성평가는 특정 위험의 영향과 발생가능성을 기준으로 다양한 정부 정책 결정을 지원하고 국가해양안보전략에서 정하고 있는 전략적 목표를 달성하기 위한 객관적 근거로 활용된다. 영국 해양위험성평가의 주요 대상은 테러리즘, 주요 해양 운송로, 주요 해양시설, 해상에서의 불법적 거래, 인신매매 및 납치 등 주요 해양 복합위협을 포함한다. 해양위험성평가의 주요 결과는 2년마다 국가위험성등록처(National Risk Register)의 위험성 평가 결과로 발간되어 범부처에서 정책결정에 활용된다.

미국 USCG MSRAM은 항만과 수로의 해양위협을 체계적으로 파악·경감하기 위해 운용되는 위험평가 체계로 USCG의 위험 관리 핵심 모델이다. USCG는 2005년에 MSRAM을 개발하여 다양한 개선을 통해 현재까지 해양위협 대응을 위한 국가 정책 결정에 활용해 오고 있다. 특히, MSRAM은 해양위협에 대응하기 위한 전략·예산·정책 결정부터 권역별 위협 예방 활동(순찰·점검·경계 활동 등)을 위한 자원 배분 등에도 활용되어 위협의 예방 및 대응 정책에 포괄적으로 적용된다. 뿐만 아니라, MSRAM은 해양 주요시설의 위험성, 주요 위험 대상에 관한 위험성을 도출하여 주요 인프라에 대한 취약성 개선 사항을 제공하기도 한다. 이는 주요 인프라의 대응력 강화 정책에 활용되어 장기적 해양 주요 인프라 개발 정책에 적용되기도 한다. 또한 MSRAM은 대부분의 데이터를 정량화하여 위협 평가에 반영하고 정성적 평가가 필요한 데이터는 현장 및 전문가 평가를 정기적으로 시행하여 결과의 객관성을 담보한다. 결과적으로 MSRAM은 상대적으로 제한된 국가 자원을 위험이 큰 곳에 배분하게 하여 자원의 효율성을 제고하고 위협을 효과적으로 억제하는 위험 기반 의사결정 체계로 USCG 관련

7월까지 적용된다. 보다 상세한 사항은 UK Government(2022.8.15.)(검색일: 2025.10.7.) 참조

정책을 지원하는 대표적 제도로 평가된다.[312]

2) 위험성 평가 제도 주요 내용

해양 복합위협 위험성 평가 제도는 평가의 대상, 방법, 결과 활용으로 구분하여 구축할 수 있다. 먼저, 위험성 평가의 대상은 우리나라 관할 해역에 위치하고 있는 무역항 및 국가중요시설, 일반 해안지역 등으로 구분하여 정하되, 주요 항만시설의 경우, 중요도에 따라 평가의 공간적 범위와 순서를 달리하고, 일반 해안지역은 해양경찰청 또는 해양 법집행기관의 효과적인 관리를 위해 관할 권역별로 구분하여 평가 대상을 설정하는 것이 필요할 것으로 판단된다.

다음으로 평가 방법은 미 USCG MSRAM 또는 영국 해양위험성평가 체계를 벤치마킹하여 우리나라 해양 특성에 적합한 평가 체계를 개발하는 것이 필요하다. 다만, MSRAM과 영국 해양위험성평가 체계는 발생가능성(빈도)과 영향(심도)의 일반적인 위험성 평가 방법을 기준으로 취약성 등을 평가 체계에 추가하여 보다 객관적이고 정량화된 평가 결과가 이루어질 수 있도록 평가 체계를 구성하고 있다.[313] 특히, MSRAM은 발생가능성 평가를 위해 공격자의 의도(Intent)와 능력(Capability)을 종합적으로 평가하고, 취약성은 공격 실현 가능성(Achievability)과 시스템 보안(System Security) 그리고 대상의 위협 방어 능력(Target Hardness)을 평가 요소로 한다.[314] 마지막으로 영향(Consequence)은 인명 피해, 경제적 손실, 환경 영향, 국가 안보 영향, 상징적 영향 등을 포함한다.

312) US Government Accountability Office(2011), pp. 27-36.
313) US Government Accountability Office(2011), pp. 19-20, 42, 50-52.
314) 보다 상세한 사항은 보 보고서 제4장 제4절과 US Government Accountability Office(2011) 보고서 참조.

〈표 5-5〉 MSRAM 평가 요소

평가 요소	위협 발생 가능성(Threat Probability)	취약성(Vulnerability)	영향(Consequence)
평가 내용	• 특정 유형의 공격이 발생할 가능성 • 정보기관의 위협 평가 자료(ICC) 기반	• 특정 자산이 해당 공격에 노출될 가능성 • 물리적 보안, 대응능력 등 현장 평가에 기반	• 공격 발생 시의 피해 수준 • 인명, 경제, 환경, 국가 안보, 상징성 등 다차원 평가 기반

자료: US Government Accountability Office(2011), p. 11 내용을 참조하여 저자 편집

마지막으로 MSRAM은 평가 요소들을 가능한 정량화하여 함수를 통한 결괏값 도출이 가능하도록 평가 체계를 구축하여 정책 결정자가 위험성을 객관적인 값을 통해 인식하도록 유도한다. 즉, MSRAM은 각각의 평가 요소를 정량화하여 함수로서 그 결과를 도출하고 있는데, 이는 확률론적 위험분석(Probabilistic Risk Assessment)의 기본 구조를 해양 보안 분야에 적합하도록 확장한 것으로 다음과 같은 수식으로 표현한다.[315]

Risk = Threat Probability × Vulnerability × Consequence

결과적으로 MSRAM 등 해양 복합위협 위험성 평가는 개별 해양위협 유형과 대상에 대한 시나리오별 위험도를 정량화하여 한정된 국가 자원의 최적 배분을 유도하고, 관련 정책의 객관적이고 투명한 기준을 확보하고, 위협 대응을 위한 전략적이고 신속한 의사결정을 지원하는 데 객관적 근거를 제공한다. 따라서 해양 복합위협 평가 방법 또한 이러한 국외 해양위협 관리 주요 국가들의 평가 방법을 참조하여 국내적으로 고도화하여 적용할 수 있을 것으로 판단된다.

마지막으로 해양 복합위협 위험성 평가 제도는 위험성 평가의 결과를 제도적으로 활용할 수 있는 분야를 정례화하여 위험성 평가의 지속가능성과 발전가능성을 확보하는 것이 필요하다. 해양 복합위협의 양태는 대상과 수

315) Ibid., pp. 8-9.

단에 따라 지속적으로 변화한다. 이에 위험성 평가의 대상과 유형 또한 지속적으로 고도화해야 하며, 이를 위해서는 위협 관리를 위한 정책 수립, 관련 기관의 역할 조정 및 강화, 대응 자원 투자, 대응 시설 및 시스템 강화 등에 위험성 평가 결과가 지속적으로 활용될 수 있도록 제도적 근거가 마련되어야 한다. 또한 중장기 해양 복합위협 대응 정책을 위해 국가 주요시설 및 권역별 해안 지역의 위험성을 정기적으로 평가하여 결과의 변화에 따라 정책을 유연화할 수 있도록 제도적 장치가 마련되어야 한다.

〈표 5-6〉 위험성 평가 결과 활용 방안

분야	내용
정책 수립	• 해양 복합위협 대응 국가 중장기 정책 수립을 위한 개별 위협의 위험성 우선순위 및 취약점 분석
국가 대응 자원 배분	• 해양 복합위협 위험 우선순위와 위협 대상 지역의 취약성을 근거로 위협 대응 자원의 합리적 배분
대응 기관 기능 조정 및 역할 강화	• 위협 대상 및 지역, 공격 수단의 위험성에 따라 관련 기관의 기능과 위치를 조정하고 주요 대응 기관의 역할을 정립
시설 및 시스템 투자	• 미래 위협 유형의 발생가능성과 위험성을 도출하여 주요시설 및 해안 지역 대응 시설 및 시스템 개선 및 투자

자료: 저자 작성

3) 위험성 평가 제도 구축 로드맵

해양 복합위협의 평가 제도는 단계적으로 위험성 평가 체계 설계, 평가 체계의 시범 적용 및 운용, 위험성 평가 제도의 법제화, 관련 정보분석플랫폼의 구축, 위험성 평가 실시로 구분하여 구축할 수 있다.

먼저 위험성 평가 체계의 설계는 앞에서 언급한 바와 같이 국외의 해양 위협 평가 제도를 참조하여 국내 해양의 특성을 고려한 평가 체계 고도화를 통해 실행이 가능하다. 이후 해양수산부, 해양경찰청, 관세청, 출입국·외국인청 등과 같이 현재 해양 복합위협에 대응하는 기관을 통해 해양 복

합위협 위험성 평가 체계를 개별 선박 및 항만 등에 적용하여 정책적으로 시범 활용하는 것이 필요하다. 이는 위험성 평가의 정책활용성을 현장에서 확인하고 실질적인 활용 범위를 확인하는 절차를 제공할 수 있다. 이후 위험성 평가의 활용 가능성을 확인한 후 해양 복합위협 위험성 제도를 법제화하는 것이 필요하다. 이를 위해 우선적으로 「해양경비법」, 「관세법」, 「국제선박항만보안법」, 「출입국관리법」 등의 하위 규정으로 '해양 (복합) 위협 위험성 평가 지침'을 도입하는 것을 고려할 수 있다. 이후 장기적으로 해양 복합위협 대응을 위한 별도의 법령이 마련되는 경우, 평가 지침을 관련 법령에 법제화하여 지속적인 운영을 위한 제도를 마련할 수 있다. 또한, 위험성 평가의 관리와 전산화를 위해 해양 복합위협 정보분석플랫폼 구축을 관련 법령에 제도화하는 것 또한 필요할 것으로 판단된다. 이는 기술적 관점에서 개별 기관에 산재되어 있는 위협 정보를 정기적으로 수집, 융합, 분석하여 위협 발생 시 즉각적인 의사결정을 지원할 수 있도록 시스템적인 보완 제도를 구축한다. 마지막으로 법제화된 위험성 평가를 실시하여 위협 대상, 지역, 공격 수단에 대한 위험 순위와 취약성을 분석하여 이를 관련 정책 및 개별 기관의 역할을 조정하는 데 활용하는 것이 필요하다.

〈표 5-7〉 해양 복합위협 위험성 평가 지침 주요 구성

구분	주요 내용	주요 내용
총칙	위험성 평가 대상	• 위험성 평가 대상을 위협 유형, 지역, 공격 수단 등으로 구분하여 규정
	위험성 평가 적용 범위	• 공간 및 유형에 관한 적용 범위 • 위험성 평가를 위한 유관기관 범위
	정의	• 해양 복합위협의 정의 및 유형
	정기적 위험성 평가	• 위험성 평가의 정기적 실시
	위험성 평가 전문가회의	• 정성 지표를 전문가를 통해 지속적으로 평가하여 시스템에 반영할 수 있도록 규정(평가 결과 환류 포함)

구분	주요 내용	주요 내용
위험성 평가 방법	위험성 평가 계획 수립	• 위협 대상, 취약점, 공격 수단 등에 따라 우선적으로 위험성 평가를 실시해야 하는 대상을 선정 • 이후 정기적 위험성 평가를 위해 대상 지역 및 해안, 주요시설을 위험순위에 따라 구분
	발생가능성	• 위협의 발생가능성을 의도, 능력 등으로 구분하여 평가할 수 있는 방법론 제시 • 정량과 정성 평가 요소를 구분
	취약성	• 공격 실현 가능성(Achievability)과 시스템 보안(System Security) 그리고 대상의 위협 방어 능력(Target Hardness)을 기준으로 평가할 수 있는 방법론 제시 • 정량과 정성 평가 요소를 구분
	영향	• 인명 피해, 경제적 손실, 환경 영향, 국가 안보 영향, 상징적 영향 등에 대해 평가할 수 있는 방법론 제시 • 정량과 정성 평가 요소를 구분
	평가 요소 현장 조사	• 평가 요소별 자료 검증을 위한 현장 조사
위험성 평가 정보 시스템 구축	정보분석플랫폼 구축 및 전산화	• 개별 대상에 대한 위험성 결과 또는 지수를 위협의 감시 및 대응에 개별 정부기관이 상시적으로 활용할 수 있도록 정보분석 플랫폼 구축 • 위험성 평가 결과의 대국민 전파
	정보협력 체계 수립	• 위험성 평가를 위한 개별 기관 정보의 상시적 정보 공유 체계 마련
평가 결과 활용 및 보존	평가 결과 활용	• 평가 결과를 웹으로 표출할 수 있도록 전산화에 대한 표준 제도 수립 • 해양 복합위협 대응 정책, 기본계획, 개별 기관 감시 및 대응 지침 마련 시 위험성 평가 결과를 참조하도록 규정
	평가 결과 보존	• 평가 결과를 표준화하여 지속적으로 활용할 수 있는 보존 방안 제시

자료: 저자 작성

제3절 정책 방안의 기대효과

1. 정책·경제적 기대효과

정책적인 측면에서 대응 방안은 국가적으로 점차 확대되고 있는 해양 복합위협을 효과적으로 관리하기 위한 제도적 방안을 수립하여 우리나라 관할 해역의 체계적 관리를 강화할 것으로 판단된다. 즉, 해양 복합위협 대응을 위한 정책적 방안은 최근 증가하고 있는 해양 영토 주권 침해 상황 등 전통·비전통 위협의 복합적 상황에 효율적으로 대응하기 위한 국가 차원의 통합적 거버넌스 모델을 제시하고 있다. 뿐만 아니라, 이러한 위협의 효과적 대응을 위한 국가전략 모델을 제시하여 통합적 거버넌스의 관리 체계와 연계하여 위협에 대응하기 위한 상위의 정책적 방향을 제시한다. 특히, 이러한 정책적 방향과 거버넌스의 합리적이고 객관적인 운용을 위해 해양 복합위협의 위험성 평가 제도를 수립하도록 제시하여, 정책 실행의 투명성과 객관성을 담보할 수 있을 것으로 판단된다.

경제적 측면에서 해양 복합위협 대응 정책 방안은 통합적 거버넌스를 통해 현재의 개별적 협력체계를 포괄적으로 관리 및 조정하는 기능을 제시하여 정부 자원의 중복성을 제거하고 효율적인 정부 기능 운용을 실현할 수 있을 것으로 판단된다. 다시 말해, 현재의 정책 방안은 해양 복합위협 위험성 평가를 통해 위험 대상, 지역, 공격 수단에 대한 우선순위 및 취약점을 분석하여 우선적으로 국가 예산이 투입되어야 하는 지역 또는 시설, 분야를 도출하여 합리적인 국가 예산 운용을 가능하게 한다. 이는 현재 개별 부처의 관할에 따라 중복적으로 투자될 수 있는 국가 예산을 절감하고 향후 효과적인 위협 대응을 위한 합리적인 국가 예산 투자가 이루어질 수 있도록 근거를 제공한다고 할 수 있다. 또한, 제시된 정책 방안은 우리 관할

해역의 안정적 이용을 촉진하여 연안지역의 경제 활동을 활성화할 수 있을 것으로 기대된다. 뿐만 아니라 우리나라 외항 국적선의 위협을 최소화하여 안정적인 글로벌 공급망 확보에 기여하여 지속가능한 국가 경제 활동을 촉진할 수 있을 것으로 기대된다.

2. 사회·기술적 기대효과

사회적 측면에서 본 연구에서 제시한 정책 대응 방안은 우리나라 관할 해역 및 우리 국적선에 대한 위협의 가능성을 최소화하여 안정적인 해양 이용과 지속가능한 해상 공급망 확보에 기여할 것으로 예상된다. 정책 방안으로 제시된 해양 복합위협 대응 국가전략은 우리나라 국익을 보호 중심으로 위협에 대응하기 위한 전략적 방향을 제시한다. 이러한 전략의 대상은 우리나라 관할 해역을 포함하여 전 세계를 항해하는 우리 국적선도 포함한다. 뿐만 아니라, 본 전략의 세부 이행 과제는 정부 부처를 포함하여 국제적인 전략 자산을 보유하고 있는 해군, 국제선박을 운영하는 해운 관계자까지 해양을 이용하는 다양한 이해관계자를 포함하여 수립되어야 한다. 따라서 본 연구에서 제시한 정책 방안은 해양위협 발생 시 민·관·군이 통합적으로 대응할 수 있는 체계를 마련하여 피해로부터의 지역사회 및 국민의 회복탄력성을 제고할 수 있을 것으로 기대된다. 또한 위험성 평가 제도 도입은 해양 복합위협 대응 정책의 투명성과 객관성을 제고하여 정책의 대국민 수용성과 신뢰성 또한 제고할 수 있을 것으로 예상된다. 마지막으로 제시된 정책 방안은 우리나라 해양 복합위협에 관한 대응력을 제고하여 향후 국제협력을 통한 국가의 위상 강화에도 기여할 수 있을 것으로 판단된다.

기술적 측면에서 본 연구의 정책 대응 방안은 정보협력 체계와 정보분석

플랫폼 구축을 제시하고 있어 위협 예방을 위한 정보 수집 및 활용, 분석에 대한 연구개발 활성화에 기여할 것으로 예상된다. 특히, 본 연구의 정책 방안은 정보분석플랫폼을 통한 정보 공유 및 분석 체계를 구축하도록 제시하고 있어, 개별 기관의 정보를 공유하기 위한 정보 표준화 기술, 감시 자원의 정보 수집 및 네트워크 기술, 정보분석을 위한 AI 활용 기술 개발 등에 기여할 수 있을 것으로 예상된다.

〈표 5-8〉 정책 방안의 기대효과

구분	기대효과
정책	• 해양 복합위협 통합 대응체계 구축→전통·비전통 위협의 효과적 대응 • 국가전략 및 위험성 평가→정책의 투명성 및 합리성 제고
경제	• 통합 대응체계 구축→개별 기관의 중복성 제거→국가 자원의 효율적 운용 및 정부 예산의 중복 투자 최소화 • 통합 대응체계 구축, 국가전략→해양의 안정적 이용 기반 마련, 안정적 해상 공급망 확보→지역사회 경제 성장, 지속가능한 국가 경제 활동 실현
사회	• 국가전략→민·관·군 통합 대응체계 마련→위협에 대한 대응력 제고 및 피해 회복탄력성 제고 • 위험성 평가 제도→정책의 투명성 및 합리성 제고→관련 정책의 대국민 수용성 및 신뢰성 제고 • 통합 대응체계, 국가전략, 위험성 평가 제도→해양 복합위협 대응력 강화→국제협력을 통한 국가 위상 강화
기술	• 위험성 평가 및 정부분석플랫폼 구축→위협 정보 표준화 기술, 위협 정보 수집 및 네트워크 공유 기술, 정보분석 AI 활용 기술 개발에 기여

자료: 저자 작성

06
결론 및 정책 제언

제1절 요약 및 결론

본 연구의 목적은 최근 변화하고 있는 해양의 위협을 분석하여 이에 효과적으로 대응하기 위한 정책적 방안을 제시하는 것이다.

이를 위해 첫째, 본 연구는 최근 해양위협의 국내외 경향과 동향을 분석하여 해양의 위협이 전통·비전통의 결합, 사이버와 연계, 동시다발적 발생으로 복합적인 양상으로 변하고 있음을 확인하였다. 그리고 본 연구에서는 이러한 최근의 위협 양상을 해양 복합위협으로 개념화하고, 위협의 대표적인 사례를 해양 국제범죄, 해양테러, 해양 사이버위협 등으로 유형화하여 조사 및 분석하였다.

해양 복합위협에 관한 논의 동향과 위협의 국내외 사례를 분석한 결과, 본 연구에서는 해양 복합위협의 양상이 점점 다양화·비정형화되고 있는 반면, 현재 관련 국내 제도·장비·협력체계는 위협에 효과적으로 대응하는 데 한계가 있음을 확인하였다.

먼저, 해양 국제범죄 사례 조사 및 분석을 통해 하나의 연속적인 사건에

서 다양한 정부 및 공공기관이 관할 구역 및 대상에 따라 분산된 기능을 수행하고 있는 것을 확인할 수 있었으며, 이렇게 개별 기관에 산재된 기능 및 역할은 단속의 사각지대 내지 책임 회피를 발생시킬 수 있음을 확인했다. 예를 들어 해양 국제범죄 중 가장 빈번히 발생하는 밀입(출)국 사건의 경우, 구체적인 상황에 대한 인지는 군, 어업인, 항만보안공사, 선장 등 다양한 주체에 의해 이루어지나 단속 등 초동 조치는 대다수 해양경찰에 의해서 이루어지고 있음을 확인했다. 사실 「국제선박항만보안법」에 따른 무역항 등 항만시설 지역의 경우, 항만공사, 지방해양수산청, 경비를 포함한 청원경찰 등이 초동 조치를 취하고, 권한 있는 기관에 사건을 인계해야 한다. 그러나 항만공사 등은 무역항 항계 내 수상구역에 대해 단속 및 대응 자원을 확보하고 있지 않아 해양경찰의 협조에 의존하고 있다. 또한 「국제선박항만보안법」이 적용되지 않는 일반 연안지역의 경우, 군 레이더 또는 해양경찰 함정을 통해 인지가 이루어지고, 해상 단속 및 초동 조치는 해양경찰이 수행하며 사건의 처리는 법무부 출입국·외국인청을 통해 이루어진다. 이는 출입국 사범의 처리에 관한 권한이 출입국·외국인청에 주어져 있으나, 해상에서의 감시 및 대응 자원을 출입국·외국인청이 보유하고 있지 않아 해양경찰의 협조를 통해 대응이 이루어지고 있기 때문이다. 다만, 이러한 협력체계는 관할과 기능에 따라 개별 기관의 요청에 의해 이루어지는 것으로 신속한 대응에 제약이 있을 수 있다. 또한, 사건의 경중에 따라 책임의 회피 내지 단속의 사각지대가 발생할 우려 또한 존재한다.

다음으로 해양 국제범죄 사례 분석 결과, 광범위한 해양에서 다양하게 발생하는 해양 복합위협을 제한된 국가 자산으로 상시적으로 감시하는 데 한계가 있음을 확인했다. 예를 들어 해상을 통한 밀수(출)입 사건은 해양경찰청과 관세청이 주로 대응하고 있으나, 관세청의 경우, 국제공항 및 항만, 통관센터, 물류거점 등에서 주된 단속을 실시하고, 기타 해상을 통한 일반 연안 지역의 밀수(출)입은 해양경찰청이 단속 및 검거를 실시한다. 특히,

관세청은 밀수 사범에 대한 처분에 관한 권한을 가지고 있는 반면, 기타 연안 및 해상에 대한 상시적인 감시 시스템을 갖추고 있지 않아, 사실상 도서 및 연안에서 발생하는 밀수 사건에 대해서는 해양경찰청의 단속 및 검거에 의존한다. 그리고 연안 및 해상에서 발생하는 밀수 사범과 관련하여서도 관세청 및 해양경찰청이 첩보를 통한 관련 범죄의 사전 인지가 부재할 시 관련 사건의 단속 및 처분은 어려운 상황이다. 더불어 밀수(출)입의 경우도 밀입(출)국과 유사하게 관세청, 해양경찰청, 항공당국, 검역당국 등이 관할 및 대상에 따라 그 역할을 구분하여 대응하고 있어 단일의 사건에 유기적이고 즉각적인 협력은 어려운 것으로 판단된다.

마지막으로 최근 국제적으로 가장 많은 논의가 이루어지고 있는 해양테러와 해양 사이버위협과 관련하여 국외 사례 조사를 통해 신흥 해양 복합위협에 대한 효과적인 대응체계가 필요함을 확인했다. 신흥 해양 복합위협은 국가 안보와 공급망에 중대한 영향을 미칠 수 있는 위협으로 최근 국제적으로 가장 많은 논의가 이루어지고 있는 분야이다.[316] 예를 들어, 최근 발생한 해저케이블 절단 및 해킹 사고, 드론 등 해상 무인체계를 활용한 선박 및 연안 주요시설 공격, 항만 및 선박에 대한 해킹 등 사이버 침해 공격은 국제 통신 체계를 일시적으로 단절시켜 국가 기능을 마비시킬 수 있고, 주요시설의 기능을 훼손하여 국가 해상 공급망에 심각한 영향을 미칠 수도 있다는 것을 확인했다. 반면, 국내적으로 이러한 신흥 해양 복합위협에 대응하기 위한 포괄적 국가 체계는 미비한 것으로 보인다. 예를 들어 2021년 한국과 중국 사이 해저케이블 절단 사고에서 과학기술정보통신부, 해양수산부, 외교부, 국내 기간통신 사업자, 해양경찰청 및 해군 등이 협력하여 사고 대응, 주변 해역 추가 위험 조사, 외교 협상, 손상 복구, 사건 조사 등을 실시했다. 다만, 이러한 협력은 개별 기관의 관할 및 기능에 따라 사건 발생 이후 사후 대응을 위해 추진되었을 뿐, 위협을 예방, 대비,

316) United Nations General Assembly, op. cit., p. 21 등 참조

대응, 복구의 전 주기로 관리하기 위한 포괄적 체계를 중심으로 수행된 것은 아니다. 현재에도 국내적으로 신흥 해양 복합위협을 상시적으로 감시하고 이러한 위협이 발생할 가능성이 있거나 발생했을 때 상황을 전파하고 효과적으로 대응하기 위한 국가적 조직 체계는 확인되지 않는다. 특히, 본 연구는 사례 분석을 통해 한 번의 해양 복합위협의 발생이 국가 안보와 국익에 막대한 영향을 미칠 수 있고, 이를 억제하기 위해서는 범부처 조직을 통해 다양한 대응 기관의 기능을 조정하고 정보분석과 사건 대응에 유기적인 협력이 필요함을 확인했다. 이는 위협을 예방함과 동시에 즉각적인 대응이 가능하도록 기능이 구축되어야 함도 확인했다.

이렇게 도출된 문제점과 협력체계 개선 필요성을 토대로, 본 연구는 둘째로 해양 복합위협을 효과적으로 관리 및 대응하고 있는 미국, 영국, 일본의 사례를 조사 및 분석하여 해양 복합위협의 실효적 대응을 위해 국내적으로 갖추어야 하는 대응체계와 제도에 대한 시사점을 도출했다. 먼저, 해양 복합위협에 대한 개별 국가의 대응체계를 요약하면 다음과 같다.

미국은 해양 복합위협과 관련하여 공공안전과 보안, 국경과 이주, 기반시설, 경제 부문을 주요 안보 위협 대상으로 분류한다. 특히, 해양에서 발생하는 위협의 주요 유형은 마약·무기, 불법 이민·납치·해적, 불응 선박, 항만 테러 등으로 구분하고 있다. 미국은 9.11테러 이후 선박과 항만에 대한 물리적 보안을 주요 법제 대상으로 두다가, 컨테이너, 세관, 외국 항만과 국제 공급망, 국제 해상화물, 해양테러, 사이버 사건 등으로 감시 및 규제 대상을 확대했다. 이러한 위협의 대응체계는 국토안보부 예하 해안경비대(USCG)를 중심으로 세관국경보호청, 이민세관단속국, 연방비상관리청이 협력하여 물자, 사람, 재난 등의 유형별 위협에 유기적으로 통합 대응하도록 구축되어 있다. 법무부 산하의 연방수사국과 마약단속국은 테러와 마약 등 조직범죄를 중심으로 조사 및 단속을 실시한다. 다만, 해상에서의 테러와 마약은 미 국토안보부 예하의 관련 기관들을 중심으로 대응하고 있으

며, 테러와 마약이 해역에서 육역으로 영향을 미칠 때, 법무부는 조사 및 단속을 위해 미 국토안보부와 유기적으로 협력한다. 마지막으로 미국은 해양작전위협대응프로토콜(MOTR)을 통해 해양 복합위협 대응 거버넌스를 구축하고 있다.

일본은 해양 이익, 해상교통로, 군사적 수단, 자연재해 등을 해양위협으로 인식하고 있다. 복합위협에 대해서는 해양에서 영토분쟁을 수반하는 회색지대 상황에 초점을 두고 있다. 주요 법제는 해상보안청법, 국제선박항만보안법, 관세법, 출입국 관련법, 테러 관련법, 사이버기본법 등이 있다. 미국처럼 사이버위협 대응을 관장하는 독립된 단일법이나 해양 사이버위협을 다루는 하위법령은 따로 두지 않는 것으로 보인다. 다만, 해양에서의 모든 위협에 대해 대응체계를 해상보안청으로 일원화하여 구축하고 있는 것이 일본의 특징이다. 즉, 해상보안청이 해역에서 발생하거나 시작되거나 영향을 미치는 모든 범죄와 위협을 관할한다.

영국은 국경, 항만, 자유항, 사이버를 해양 복합위협 대응을 위한 주요 관리 대상으로 정하고 있다. 즉, 수역, 항만과 선박, 글로벌 해운 항로에서 발생하는 해양 범죄와 해적, 테러, 사이버위협 등을 주요 위협으로 고려하고 있다. 주요 법제는 해양항해법, 관세법, 망명·이민·이주 관련 법, 안보·테러 관련법, 사이버보안·복원법(법안 제출 예정) 등이 있다. 대응체계는 유관기관의 역할이 제도적으로 결합되어 있다. 해양경비청(정보 입수)-국경수비대(검문·단속)-국가범죄청(수사) 순으로 역할이 맞물려 있으며, 물자에 대해서는 세관 및 국세청, 형사 고발에 대해서는 검찰기소청으로 업무가 유기적으로 연계되어 있다. 해양 복합위협 대응 거버넌스로는 합동해양안보센터와 합동해양작전조정센터 등을 구축하고 있다. 특징적인 것은 영국의 경우, 대응 기관의 기능에 따라 권한과 책임이 명확히 구분되어 있어 관할의 중첩이나 대응의 사각지대를 최소화한다는 것이다.

이에 본 연구에서는 미국은 해안경비대(USCG)를 비롯해 세관국경보호청·이민세관단속국을 산하에 둔 국토안보부를 중심으로 통합된 대응체계를 구축하고 있다는 것을 확인했다. 그리고 일본은 해상보안청이 대부분을 전담하면서, 출입국재류관리청, 세관과 관련 업무를 연계하는 것으로 확인했다. 마지막으로 영국은 해양경비청, 국경수비대, 세관 및 국세청, 국가범죄청 등으로 기능을 분화시켜 기관 간 유기적인 연대를 강화하고 있는 것을 확인했다. 즉, 미국은 유관기관 간의 역할이 고도로 통합되어 있고, 영국은 다기관에 기능을 구분하여 유기적인 협력을 제도적으로 갖추고 있으며, 이를 통해 권력의 분산을 도모하고 있으며, 일본은 명확한 권한을 명시함으로써 실행 권력을 중심으로 대응체계를 일원화하고 있는 것을 확인할 수 있다.

다음으로 본 연구는 국내 대응체계를 해양 복합위협 유형별로 살펴보고, 앞서 검토한 국외 대응체계와 비교하여 개선 사항을 도출했다. 먼저, 본 연구는 해양 국제범죄에 대한 국내 대응체계가 관할 및 대상별로 위협의 단속과 처리에 대한 책임과 권한을 기관별로 분산하여 운영하고 있어, 위협에 대한 연속적이고 효과적인 대응에 한계가 있는 것으로 확인했다. 이는 국외에서 해양의 위협을 일원화 또는 통합적으로 대응하는 것과 달리 하나의 연속적인 위협 행위를 여러 기관이 관할에 따라 요청에 의해 단절적으로 대응하는 것을 의미한다. 예를 들어, 육상에서 항만을 통해 선박을 이용하여 국외로 밀항하는 경우, 위협 행위가 공간적 범위에 따라 대응 기관이 출입국·외국인청(육상)→해양수산부(항만공사)(항만)→해양경찰청(항계 밖 해상) 등으로 변경된다. 이러한 경우, 사건의 인계 및 기관의 역할 전환 내지 협조가 시의적절히 이루어지지 않는다면, 대응의 공백 내지 사각지대가 발생하여 위협의 최종 실현으로 귀결될 수 있다. 또한 이러한 권한의 분산은 관할이 전환되는 시점에 기관 간 권한의 중첩을 발생시킬 가능성 또한 있고, 권한의 중첩은 기관 간 책임 회피로 연결될 수도 있다. 예를 들어,

항만의 수상구역에서 해양경찰의 위법행위 단속 권한과, 해양수산부 내지 항만공사의 보안관리 권한, 그리고 연안 지역에서 출입국·외국인청의 출입국 사법에 관한 단속 권한과 해양경찰의 밀입국자 단속 권한 등은 동일한 관할 구역에 중첩해서 존재한다. 이러한 권한의 중첩은 사건에 따라 자칫 대응 기관의 책임 회피로 연결될 수 있어 개별 사건에 따라 이러한 재량에 따라 공조 내지 협력하기보다 이를 제도화하여 유기적인 협력이 이루어지도록 해야 한다. 결국 권한과 책임의 분산에서 오는 한계를 극복하기 위해서는 위협의 효과적 대응을 위한 통합적 대응체계를 구축하여 관련 기관의 권한과 기능을 상시적으로 조정할 수 있도록 해야 하며, 특히 다양한 기관의 권한 및 책임을 관할 및 대상에 따라 지침 등으로 제도화하여 유기적인 협조 내지 공조가 가능하도록 해야 한다.

해양 국제범죄 대응체계와 달리 해양테러와 해양 사이버위협에 관한 국내 대응체계는 상대적으로 통합적 접근을 시도하고 있는 것으로 보인다. 다만, 현재의 해양테러와 국가 사이버위협 대응체계는 국가행위자의 회색지대 위협, 해저케이블 훼손, 무인체계 활용 공격 등 신흥 해양 복합위협에 대응하는 것에는 한계가 있는 것으로 확인된다. 특히, 「테러방지법」은 해양테러의 정의와 범위를 별도로 규정하고 있지 않아 테러 행위가 해양에서 시작하여 종국적으로 육상 주요시설의 공격으로 귀결될 때, 이를 어떤 기관이 주관하여 담당해야 하는지 그 역할이 분명하지 않을 수 있다. 또한 국가사이버안보 체계와 관련하여 해양분야 주무 부처가 해양수산부로 명시되어 있으나, 이는 해사·항만분야 사이버보안 강화에 관한 정책에 한정하고 있는 것으로 보인다. 즉, 국가사이버안보 체계에서 자율운항시스템, 항만 시스템 해킹 등 해양 사이버범죄 대응에 관한 사항은 누락되어 있어 이를 보완하기 위한 정책 개발 내지 협력이 필요한 것으로 확인된다.

본 연구는 또한 앞에서 도출된 국내 대응체계의 취약점과 개선사항을 고려하여, 우선적으로 대응해야 하는 해양 복합위협을 확인하기 위해, 해양

국제범죄 통계를 변동성과 시계열을 중심으로 분석했고, 대응 기관의 위치와 범죄 발생 간의 관계를 확인하기 위해 GIS 분석을 실시했다. 또한 국내 관할 해역에서 향후 우선적으로 대응해야 할 해양 복합위협을 확인하기 위해 위험성 분석 또한 실시했다.

먼저, 해양 국제범죄 통계의 변동성 분석을 통해 본 연구는 우리 해역에서 가장 우선적으로 대응해야 하는 위협이 밀입(출)국 및 밀항 등과 관련된 출입국문란 범죄와 밀수(출)입 등과 관련된 관세 범죄로 확인했다. 특히, 이들 해양 국제범죄에 대응하기 위해서는 단기적으로 범죄 발생을 억제 및 관리하기 위한 발생 원인 분석과 현 국가 자원의 효과적 활용이 필요함을 확인할 수 있었다. 그리고 장기적으로 범죄의 변동성을 관리 및 대응을 위해서는 범죄의 경향, 동향, 원인 등을 다층적으로 분석하여 대응 조직, 자원 등을 적절히 배분하는 정책적 대응 방안 또한 수립되어야 하는 것을 확인했다.

다음으로 본 연구는 해양 국제범죄의 GIS 분석을 통해 해양 복합위협 관리 및 대응을 위한 정보 공유 부족, 해상 및 도서 등 육지에서 원거리에 위치한 범죄 대응 자원 부족, 복합위협의 발생의 불확실성을 확인할 수 있었다. GIS 분석은 지난 5년(2021년~2024년) 발생한 해양 국제범죄 중 해양경찰청에서 관리하고 있는 통계를 중심으로 분석을 실시했으며, 해양 국제범죄 발생 핫스팟 분석, 관련 기관의 위치와 범죄 발생 위치와의 상관관계, 해상교통량과의 범죄 발생 위치와의 관계를 통해 분석했다. 특히, 범죄 발생 핫스팟 분석과 범죄 발생 위치 분석을 통해 개별 범죄 유형에 따라 관련 기관의 협력이 범죄 예방 및 대응에 필수적임을 확인할 수 있었다. 보안사고 등 해양수산부와 관련된 범죄는 주로 부산 지역, 출입국 사범 등 출입국·외국인청과 관련된 범죄는 군산 및 제주 등 주로 서해 또는 제주 먼바다, 식품안전 사범 등 지방식품의약품안정청과 관련된 범죄는 주로 목포 등 섬 지역, 마약 밀수 사범 등 관세청과 관련된 범죄는 주로 부산 지역

에서 발생한 것으로 확인되었다. 해양 국제범죄 유형에 따라 발생 위치가 상이하고, 최종 처분 기관을 달리하고 있어 이를 통합적으로 관리하는 체계가 필요함을 확인할 수 있다. 특히, 해양경찰청의 경우, 발생하는 이들 모든 위협에 대해 일반사법경찰기관으로 초동 조치를 취해야 하는 의무와 책임을 가지고 있다. 또한, 해양경찰청은 해상에서 실효적으로 단속할 수 있는 유일한 능력과 자원을 가지고 있는 기관으로 관계기관과의 정보 및 첩보에 대한 협력체계가 필수적으로 구축되어야 함을 확인할 수 있었다. 또한 본 연구는 해상교통량과 범죄 발생 위치와의 분석을 통해, 제2장의 해양 복합위협의 불확실성이 우리나라 관할 해역에서도 나타남을 확인할 수 있었다. 즉, 사고 등 우발적으로 발생하는 해양환경 오염 범죄를 제외하고 대다수의 범죄가 일반적인 해상교통의 흐름에서 벗어나서 발생하는 것을 확인할 수 있었다. 이에 해양 국제범죄의 효과적인 대응을 위해서는 민·관·군·경 등의 자산을 통합적으로 활용하여 위협을 협력적으로 관리하는 범정부 체계가 필요하다는 것을 확인할 수 있었다.

또한, 본 연구에서는 미래 해양 복합위협 분석을 위해 위협에 대한 전문가 설문 및 자문을 통해 향후 우리나라 관할 해역에서 발생가능한 위협의 위험성을 분석하고 이에 대한 정책적 시사점 또한 도출했다. 먼저, 해양 복합위협 위험성 분석을 기준으로 드론 공격, 해저시설 공격, 사이버위협 등 신흥 해양 복합위협에 대한 위협 대응 전 주기에 걸친 대응 정책 및 제도적 수단이 마련되어야 하는 것으로 분석되었다. 밀입(출)국 및 밀수(출)입에 대해서도 예방 및 대비를 위한 정책이 우선적으로 마련되어야 하는 것으로 분석되었다. 특히, 신흥 복합위협의 경우, 제2장의 사례와 제3장의 국외 사례에서도 확인하였듯, 하나의 개별 기관의 대응보다, 국가 자원 및 기능에 따라 범부처 협력체계를 통한 통합적 국가적 대응체계가 마련되어야 하는 것으로 판단된다. 또한 이러한 위협은 일단 발생하면 국가 안보와 국익 전체를 위험에 빠뜨릴 수 있어 이에 대응하기 위한 국가 차원의 전략 체계

또한 마련되어야 하는 것으로 판단된다. 밀입(출)국 및 밀수(출)입의 경우, 일부 위협 유형에 대해서는 협의체가 구성되어 있으나, 이를 포괄적으로 예방 및 대비하기 위한 협력체계가 부족한 것으로 판단된다. 즉, 밀입(출)국 및 밀수(출)입의 효과적 예방 및 대비를 위해서는 이들 위협에 대한 상시적인 감시와 기관 간 정보 공유 체계가 필수적인 반면, 국내적으로 기관 간 상시적인 정보 공유 및 분석 체계는 미흡한 것으로 판단된다. 이에, 이들 위협에 대한 효과적인 대응을 위해서 위협에 대한 상시 감시체계를 보완하는 한편 이들 위협의 흐름에 대한 정보를 기관 간 공유하는 것이 필요한 것으로 확인되었다.

이러한 분석과 시사점을 중심으로 본 연구는 다음과 같이 세 가지 정책적 대응 방향을 제시했다. 첫째, 현재 분절적으로 운영되고 있는 국내 대응체계의 개선과 범부처를 통한 통합적 대응체계의 구축이다. 이는 책임의 경계가 모호한 해양 복합위협에 효과적으로 대응할 수 있도록 기관 간 기능과 역할을 조정하여 책임을 명확히 하고 한정된 자원을 효율적으로 운영하여 발생하는 위협에 실질적으로 대응할 수 있는 대응체계 마련을 의미한다. 둘째, 신흥 해양 복합위협으로부터 국익과 해양안보를 효과적으로 보호하기 위한 국가전략의 수립이다. 신흥 해양 복합위협은 한 번의 발생으로 글로벌 공급망 위기, 또는 국익의 막대한 손해 등으로 연결될 가능성을 다분히 가지고 있다. 반면, 이러한 위협의 다양한 형태와 불확실성은 기능상 하나의 부처만으로 효과적인 대응을 기대하기는 어렵다. 이에, 위협을 유형화하여 위험성을 평가하여 새로운 위협에 대해서도 다양한 부처의 기능이 유기적으로 연결될 수 있도록 국가적인 지침 및 전략을 개발해야 한다. 이를 위해서 국가전략은 통합적 거버넌스, 정보의 통합을 위한 정보분석플랫폼 구축, 위협에 대한 위험성 평가 제도, 지역 및 국제 공조 제도화를 주요 내용으로 구성할 수 있을 것으로 판단된다. 마지막 셋째, 통합적 대응체계 및 해양 복합위협 대응 국가전략을 효과적으로 운영하기 위한 위험성 및

취약성 평가 제도의 마련이다. 즉, 제한된 국가 자원으로 해양 복합위협을 효과적으로 억제 및 대응하기 위해서는 위협 유형 및 대상의 위험성 내지 발생가능성을 객관적으로 평가하여 우선순위에 따른 대응체계를 수립하고, 개별 대상의 취약성을 중심으로 필수적인 장비 및 시스템을 구비해야 할 것으로 판단된다.

제2절 정책 제언

1. 통합적 거버넌스 및 국가전략의 제도화

해양 복합위협의 대응을 위한 통합적 거버넌스는 제도적인 근거와 국가전략이 함께 구축될 때 효과적으로 운영될 수 있다. 최근 해양위협의 양상은 사이버 수단과 연계하여 연결성과 복잡성을 더하고 있으며, 행위자의 인지가 어렵고, 피해가 동시다발적으로 발생하여 다양한 기관의 협력적인 대응이 필요하다. 뿐만 아니라 광범위한 관할 해역과 해양위협의 다양화는 단일 부처 내지 기관의 대응만으로 사실상 효과적인 위협 억제 효과를 기대하기 어렵게 한다. 이에 본 연구에서는 최근 해양위협의 복합적인 양상을 해양 복합위협으로 개념화하고 이에 효과적으로 대응하기 위한 정책 방안으로 통합적 대응체계 구축 및 해양 복합위협 대응 국가전략 구축을 제시하고 있다. 즉, 국가적 해양 복합위협을 실효적으로 대응하기 위한 통합적 거버넌스를 제도적으로 구축하고 이를 이행하기 위한 국가전략을 수립하여 지속가능하며 효과적인 협력적 대응체계를 구축해야 한다는 것이다. 이는 하나의 해양 복합위협이 국가 안보와 국가 기능에 막대한 영향을 미칠 수 있는 것을 고려하여 위협을 예방부터 복구까지 전 주기로 관리하는

체계를 구축하는 것을 의미한다.

먼저, 해양 복합위협 대응을 위한 국가전략은 국가적 해양위협에 대응하기 위한 국가 자원의 이용 및 기관 간 협력체계를 상위 전략으로 제시하고, 장기적으로 통합적 거버넌스의 효과적 운영을 위한 제도적 대응체계를 마련할 수 있도록 정책 방향을 제시해야 한다. 이를 위해, 국가전략은 해양 복합위협에 위험성과 중대함을 인식하고 이에 효과적으로 대응하기 위한 상위 개념의 거버넌스 체계를 제시해야 한다. 특히, 상위 개념의 통합적 거버넌스는 민·관·군·경을 포함해 다양한 이해관계자가 각 기능 및 역할에 따라 위협을 유기적으로 대응할 수 있도록 협력체계를 개념화하여 제시해야 한다. 국가적 해양 복합위협에 대해서는 상위의 기관이 개별 기관의 역할과 책임을 조정하여 대응과 자원의 중복성을 제거하여 효율적이고 즉각적인 위협 대응이 이루어질 수 있도록 일정한 시행 지침 또는 안내서가 마련되어야 한다. 또한 발생가능성이 높은 해양 복합위협에 대해서는 상시적인 대응체계를 통해 실질적인 위협 억제가 이루어질 수 있도록 제도적 장치 마련에 대한 전략이 수립되어야 한다. 뿐만 아니라 국가전략은 해양 복합위협의 대상 및 유형에 따라 지역 및 국제적으로 협력이 필요한 분야를 구분하고 다양한 이해관계자를 고려한 전략적 협력이 이루어질 수 있도록 장기적 국제협력 전략 또한 제시해야 한다.

다음으로 해양 복합위협 대응체계는 이러한 국가전략을 책임지고 관리 및 이행하는 동시에, 발생가능성이 높은 해양 복합위협을 상시적으로 대응할 수 있는 국가 체계를 제도적으로 마련하는 것을 의미한다. 특히, 최근 발생하고 있는 다양한 위협들은 기관별 소관 법령에 따라 분절된 권한 및 책임으로 위협의 단절적 대응 내지 사각지대를 발생시킬 수 있다. 뿐만 아니라 제한적이기는 하나, 개별 기관의 관할 및 기능의 중첩은 해양 복합위협에 대한 책임 회피 가능성을 내포하고 있다. 따라서 이러한 단절적 대응과 책임 회피 가능성을 최소화하기 위해서는 발생가능성이 높은 해양 복합

위협에 대한 개별 기관의 권한 및 책임을 상시적으로 조정할 수 있는 범부처 대응체계가 필요하다. 이를 위해서 '국가해양위협대책위원회'(가칭) 등과 같은 위협에 대응하는 상설 기능 조정위원회를 설립하는 것이 필요하며, 이를 통해 해양 복합위협 대응 국가전략을 수립, 관리, 이행하는 제도적 장치를 마련하는 것이 필요할 것으로 판단된다.

2. 해양 복합위협 위험성 평가 및 정보분석플랫폼 구축

해양 복합위협 국가전략과 대응체계의 효과적 운영을 위해서는 해양 복합위협을 정량적으로 평가할 수 있는 제도적 장치와 평가 정보를 포함한 위협의 예측 및 예방을 위한 정보분석플랫폼의 구축 또한 필요하다.

먼저, 해양 복합위협 평가를 위한 제도적 장치는 국외 사례 등을 고려하여 해양 복합위협 위험성 평가 제도로 개발할 수 있다. 특히, 이러한 평가 제도는 평가의 대상, 방법, 결과 활용으로 구분하여 구축할 수 있을 것으로 판단된다. 위험성 평가의 대상은 우리나라 관할 해역에 위치하고 있는 무역항 및 국가중요시설, 일반 해안지역 등으로 구분하여 정하되, 주요 항만시설의 경우, 중요도에 따라 평가의 공간적 범위와 순서를 달리하고, 일반 해안지역은 해양경찰청 또는 해양 법집행기관의 효과적인 관리를 위해 관할 권역별로 구분하여 평가 대상을 설정할 수 있다. 평가의 방법은 미 USCG MSRAM의 정보 수집 기법과 정량화 기법 등을 참조하여 개별 해양위협의 유형과 대상, 그리고 공격 수단을 중심으로 시나리오를 개발하여 위협 발생가능성(Threats Probability), 취약성(Vulnerability), 영향(Consequence)을 정량화하여 위험성을 도출하는 방식을 고려할 수 있다. 다만, 개별 요소의 정량화를 평가 기준은 국내 환경을 고려한 별도의 방법론 개발이 필요할 것으로 판단된다. 마지막으로 위험성 평가의 결과는 위

협의 지역, 대상, 유형에 따라 위협 대응 정책을 예방, 대비, 대응, 복구 4단계로 구분하여 단계별로 수립할 수 있는 정책의 우선순위를 결정하는 근거 자료로 활용할 수 있을 것이다. 특히, 다양한 관계부처가 위협 대응에 관련되는 국내 환경을 고려하여 위협 대응 정책이 관련 기관의 기능을 조정하여 효과적으로 대응할 수 있도록 하는 근거 자료로 활용할 수 있을 것으로 판단된다.

다음으로 해양 복합위협의 효과적 예방 및 대비를 위해, 현재 다양한 기관에 분산되어 관리되고 있는 해양 복합위협에 관한 정보를 하나의 정보분석플랫폼을 통해 분석 및 공유할 수 있도록 구축하는 것이 필요하다. 이를 위해서는 해양 복합위협을 유형화하고 위협의 예측 및 대응을 위한 필요 정보를 도출하는 것이 필요하다. 이를 통해 관련 국가전략 내지 관련 제도를 통해 기관들이 공유해야 하는 정보를 제시하고 위협 유형에 따라 분석된 결과를 공유하는 체계 또한 제시하는 것이 필요하다. 특히, 위협을 예방하기 위한 정책 결정자, 위협에 대응하기 위한 해양 법집행기관에 정보가 효과적으로 공유될 수 있도록 정보분석플랫폼의 관리 체계가 구축되어야 하고, 정보의 비인가 전파를 막기 위해 정보의 단계별 관리 체계 또한 구축되어야 한다. 이러한 정보분석플랫폼의 설치는 앞서 언급한 국가해양위협대책위원회 예하에 이루어질 수 있을 것으로 판단되며, 이를 통해 기관별로 분산된 정보로 인한 위협의 단절적 대응 내지 사각지대가 최소화될 수 있을 것으로 판단된다. 또한, 국가해양위협대책위원회는 포괄적 정보분석 및 운영을 통해 개별 기관의 기능을 효율적으로 운용할 수 있는 근거 자료를 마련할 수 있을 것으로 판단된다.

제3절 후속과제

1. 해양 복합위협 관련 정보 수집 및 관리 체계 구축 연구

본 연구는 우리나라 관할 해역에서 발생하는 해양 복합위협 현황과 관련 기관의 역할 및 배치를 분석하여 현행 위협 대응체계의 한계를 분석하고 해양위협의 변화 양상에 따른 대응 방안을 제시하고자 하였다.

다만, 이러한 목적에도 불구하고 현재 국내에는 전통적 해양위협인 밀입(출)국, 밀수(출)입 등을 포함하여, 신흥 해양 복합위협인 해저 시설 공격, 해양 사이버위협 등에 관한 상세한 현황 정보 관리 체계가 구축되어 있지 않아 해양 복합위협의 경향성 분석 및 GIS 분석에 상당한 제약이 있었다. 특히, 개별 기관에서 관할에 따라 관리하고 있는 사건 통계가 상이하거나 중복적으로 계수되는 경우 또한 발견할 수 있었다. 그리고 사건 발생 위치가 연속적으로 변경되거나 사건의 인지가 발생 이후 일정한 시간이 지난 뒤 이루어진 경우, 사건의 발생 위치와 인지 위치가 구분되지 않는 경우도 있었으며, 사건 위협의 발생 위치가 범죄로서 귀결되는 위치와 상이할 때 사건의 발생 위치를 어느 기준으로 해야 하는지 모호한 경우도 있었다. 또한 해양 국제범죄 GIS 분석을 위해 활용된 위치정보는 범죄 정보로서 개인정보로 인한 활용에 제한이 있었고, 따라서 범죄 발생 핫스팟 분석 및 관계성 분석에 있어 위치상 상당히 오차가 내포되어 있다. 이에, 해양 국제범죄 GIS 분석은 사실상 정책 수립을 위한 참조로만 활용이 가능할 것으로 판단되며, 지역별 범죄대응을 위한 구체적 대응 방안 마련에는 참고하기 어려울 것으로 판단된다. 마지막으로 신흥 해양 복합위협에 대해서는 관련 법체계가 마련되어 있지 않아 해양 국제범죄로서 관리되고 있지 않을 뿐만 아니라, 별도의 통계 관리 체계로도 확인이 어려워 사실상

접근이 어려웠다.

따라서 향후 후속연구에서는 해양 복합위협이 지속적으로 증가하는 것을 고려하여 국내 해양 복합위협을 유형화하고 분류하여 통계적으로 관리하는 체계를 구축할 수 있도록 연구할 필요가 있다. 특히, 「테러방지법」 등을 참조하여 테러에 관한 정보, 수집, 분석, 관리 운용 체계 등을 분석하고, 해양에서 발생하는 위협의 정보를 발생 위치, 위협의 수준 등 단계별로 구분하여 관리, 분석, 전파하는 체계 도입을 상세하게 연구할 필요가 있다. 현재 국방부, 해양경찰청, 해군 등은 향후 우리나라 관할 해역을 포함하여 우리나라 국적선이 항해하는 전 세계해역에서 발생하는 위협을 최대한 상시적으로 감시하고 분석하기 위한 해양영역인식(MDA: Maritime Domain Awareness) 체계를 개발하고 있다. 특히, MDA 체계는 구축하고 있는 기관에 따라 수집하는 정보는 유사하나 활용 목적이 달라 정보분석의 틀이 상이하고 수집 정보의 깊이가 다를 수 있다. 이에, 기관에 따라 MDA를 통해 수집하는 정보를 협력적으로 관리 및 분석하는 체계에 대해 향후 구체적으로 연구할 필요가 있는 것으로 판단된다.

2. 해양 복합위협 위험성 평가 모델 개발 연구

본 연구는 또한 해양 복합위협의 위험성을 평가하여 정량적인 결과를 통해 위협의 우선순위를 분석하고, 이를 통해 정책적 시사점을 개별 유형 및 대상에 따라 구체적으로 도출하고자 했다.

그러나 상당한 기간 동안 해양위협 평가 제도를 운영하여 고도화한 미국 및 영국 등 선진국과 달리, 국내에는 해양 국제범죄를 포함하여 해양에서 발생하는 복합위협의 위험성을 구체적으로 평가하는 제도 내지 지침이 부재하여 평가를 위한 수치화된 정보를 확보하기 어려웠다. 특히, 미국 등 위

험성 평가 주요 선진국들은 정성적인 평가 요소를 최소화하고 위협의 경제적 피해, 사상자 등 인구·사회학적 영향, 위협의 범위, 위협 장비 및 시설의 수준, 공격 수단의 성능과 영향 등을 수치화하여 위험성 평가가 최대한 객관적 자료로 정량화되도록 설계하고 있다. 반면, 국내에는 위협과 관련된 통계학적 정보를 유효하게 관리하고 있는 통계 관리 정보 체계가 구축되어 있지 않으며, 해양 복합위협과 관련된 대부분의 통계자료는 대다수 대외비로 외부 공개가 제한되어 있다. 이에 본 연구에서 진행한 위험성 평가 또한 모든 요소를 전문가 설문을 통해 진행했다. 이에, 본 연구에서 진행된 위험성 평가는 모든 요소가 정성적으로 평가되어 전문가 설문 대상에 따라 결과의 변동성이 있을 것으로 판단된다. 다만, 본 연구는 위험성 평가의 객관성과 전문성을 담보하기 위해 출입국·외국인청, 해양경찰청, 해양수산부, 항만공사 등 실제 위협 대응 업무에 종사하고 있는 전문가를 설문 대상으로 섭외했다.

따라서 후속 연구에서는 보다 정량적인 위험성 평가를 통한 해양 복합위협 대응 정책 개발을 위해 해양 복합위협 위험성 평가를 위한 구체적인 체계와 방법론을 개발하는 것이 필요할 것으로 판단된다. 특히, 이러한 위험성 평가 체계는 우리나라 지정학적 환경, 해양 여건, 연안 환경, 관련 기관의 역할 및 위치, 국가 자원 등을 고려하여 국내적으로 적용할 수 있도록 개발되어야 할 것으로 판단되며, 이를 위해 미국, 영국, 호주 등에서 현재 적용하고 있는 해양위협 평가 제도를 면밀히 분석할 필요가 있다.

참고문헌

국내 문헌

관계부처 합동(2024), 2024 국가 사이버안보 기본계획, 국가사이버안보센터.

국무조정실 대테러센터(2023), 국가중요시설 및 다중이용시설에 대한 테러예방대책 업무편람.

국정기획위원회(2025), 국민보고대회 발표 자료.

김소정(2024), 하이브리드 위협 대응을 위한 정책 고려사항, 이슈브리프, 612, 국가안보전략연구원.

김재광(2019), 항만 등 국가중요시설 민간경비체계의 법적 문제와 개선방안, 공법학연구, 20(1), pp. 47-77.

김재운(2014), 해양범죄의 수사역량 강화를 위한 해양경찰 수사교육전문화에 관한 연구, 디지털융복합연구, 12(6), pp. 35-42.

김찬호·최건우·박상원(2017), 항만보안 관리체계 효율화 방안 연구, 한국해양수산개발원.

노호래(2022), 해양경찰학개론

류재학·허지용·나윤후(2023), 미래전 활용을 위한 해양무인체계 발전전략에 관한 연구, 한국해군과학기술학회지, 6(2), pp. 127-132.

박경규 외(2023), 특별수사기관의 수사체계 안착방안 연구(II) - 해양경찰을 중심으로, 형사정책연구원 연구총서, 한국형사법무정책연구원.

박민석 외(2024), 육군 위험성평가체계의 사고예방효과에 관한 연구, 한국산업경영시스템학회지, 47(2), pp. 84-92.

박성수(2018), 마약류 등 유해약물의 사회적 비용 분석, 치안정책연구, 32(3), pp. 217-253.

박성수·백민석(2019), 마약류 범죄의 암수율 측정에 관한 질적 연구, 한국경찰연구, 18(1), pp. 151-170.

박용기(2006), 미국 테러방지법의 현황 및 주요내용 - 우리 테러방지법제 정비방안 검토, 서울중앙지방검찰청 해외연수 검사 논문.

박주상·박동균(2010), 국제해양범죄에 대한 해양경찰의 효율적 대응방안, 한국치안행정논집, 7(3), pp. 66-88.

반길주(2025A), 중국의 서해 구조물 설치와 회색지대전략: 양상 및 방책, IFANS FOCUS, 국립외교원 외교안보연구소.

반길주(2025B), 해저케이블 안보와 회색지대 공세, 국가안보와 전략, 25(1), pp. 157-184.

방호삼·하민재(2022), 해양 선박재난 대응을 위한 거버넌스 법제 연구, 해양환경안전학회지, 28(2), pp. 334-345.

송태은(2020), 하이브리드 위협에 대한 최근 유럽의 대응, 주요국제문제분석, 2020-31, 국립외교원 외교안보연구소.

신소현·임정희(2025), 해저케이블 사보타주에 대한 국제사회의 대응과 한국에 대한 시사점, 아산정책연구소.

신용도·조홍제(2018), 외로운 늑대형의 국내테러에 관한 연구, 한구테러학회보, 11(3), pp. 49-64.

유재두·노호래(2018), 해양 밀입국 실태와 해양경찰의 대응방안, 한국해양경찰학회보, 8(1), pp. 129-143.

윤봉한·이상진·임종인(2015), 국내에서의 '외로운 늑대'(Lone Wolf) 테러리스트 발생 가능성에 관한 연구: IS 가담 '김 모'군의 사이버 공간에서의 행적을 중심으로, 한국전자거래학회지, 20(4), pp. 127-150.

이서항(2023), 또다시 떠오르는 중국의 '세계적' 불법조업 문제, KIMS Periscope, 305, 한국해양전략연구소.

이순태·이유봉(2017), 해양의 안전관리를 위한 법제 개선방안 연구, 한국법제연구원.

이종화(2003), 국제범죄의 개념과 현황, 한국경찰법연구, 1(1), pp. 194-213.

정아신·양쥔·조정형(2024), KANO 모델을 활용한 연안 지역의 CPTED 수요 분석 – 부산광역시 미포마을을 중심으로 -, 한국디자인리서치학회지, 9(2), pp. 84-93.

정현욱(2025), '살라미 전술'의 시작?: 서해 구조물에 투영된 중국의 안보전략, Issue Brief, 683, 국가안보전략연구원.

정현욱·김소정(2025), 해저케이블 절단의 안보적 위협: 순싱39호의 대만 해저케이블 절단 사례, Issue Brief, 649, 국가안보전략연구원.

조민상(2023), 해양에서의 밀입국·밀출국 특성과 대응방안, 한국민간경비학회보, 22, pp. 209-226.

채성준(2016), 국제범죄의 개념 정립 및 효율적 대응방안 연구, 국가정보연구, 9(2), pp. 295-326.

최석윤·최정호(2016), 해상사건 수사 직무 범위에 관한 연구, 한국경찰연구, 15(4), pp. 235-262.

하도연·김율성(2023), 부산항 컨테이너 터미널 사이버 보안 강화를 위한 탐색적 연구, 한국항해항만학회지, 47(6), pp. 437-447.

한국해양수산개발원(2025.5.12.), 해양 국제범죄 데이터(내부자료).

한재진·최정호(2020), 한국 해양경찰청과 일본 해상보안청의 국제해양범죄수사기능 비교 및 시사점, 한국해양경찰학회보, 10(2), pp. 81-108.

함혜현(2022), 해양 대테러 정보활동 발전방안 연구, 한국해양경찰학회보, 12(1), pp. 173-197.

함혜현·전봉조·이장욱(2022), 항만보안 관할권 소재에 관한 법적 고찰 - 항만 보호구역 내 해상구역을 중심으로 -, 한국공안행정학회보, 87, pp. 371-398.

해양경찰청(2025), 해양 국제범죄 발생 현황(내부자료).

해양경찰청(2025.3.25.), 미국 및 일본 현황(내부자료).

해양경찰청(2025.4.18.), 연구 관련 질의 응답(내부자료).

해양수산부(2025), AIS 화물선 데이터(내부자료).

현대중공업(주)(2014.1.14.), KR-A-10-2014-0004893.

국외 문헌

Australian Government(2021), Australian Government Civil Maritime Security Strategy.

Australian Government(2020), Guide to Australian Maritime Security Arrangements(GAMSA).

Downs, Brady, LCDR(2008), Maritime Security Risk Analysis Model(MSRAM) Balancing resources to risk, Presentation for the Critical Infrastructure Protection Workshop, The Center for Homeland Defense and Security. USCG.

Department for Transport(2019), Maritime for 2050: Navigating the Future.

Department of Homeland Security(2024), Homeland Threat Assessment 2025.

Department of Homeland Security USCG(2013), USCG Addendum to the United States National Search and Rescue Supplement.

EMODnet,(2019.3.), EU Vessel density map Detailed method, The European Marine Observation and Data Network.

Federal Emergency Management Agency (FEMA)(2017), National Incident Management System, 3rd Edition, US Department of Homeland Security.

Federal Emergency Management Agency (FEMA)(2016), Emergency Support Function #9 – Search and Rescue, US Department of Homeland Security.

Federal Maritime Commission(2024.2.25.), Demurage and Detention Billing Requirement 46 CFR Part 541, Federal Register, 89(38), pp. 14330-14363.

Gülcan, Tolga Ahmet, & Erginer, Kadir Emrah(2023), National and International Maritime Situational Awareness Model Examples and the Effects of North Stream Pipelines Sabotage, International Journal of Critical Infrastructure Prootection, 42, 100624.

HM Treasury(2020), Freeports Bidding Prospectus.

HM Government(2022), National Strategy for Maritime Security.

HM Government(2025), National Risk Register.

Home Office(2020), Examining Officers and Review Officers under Schedule 3 to

the Counter-Terrorism and Border Security Act 2019.

Hybrid CoE(2025), Protecting maritime infrastructure from hybrid threats: legal opt ions, The European Centre of Excellence for Countering Hybrid Threats.

Hybrid CoE(2023), Handbook on maritime hybrid threats: 15 scenarios and legal scans, The European Centre of Excellence for Countering Hybrid Threats.

Larsson, Oscar L., & Widen, J.J.(2024), The European Union as a Maritime Security Provider – The Naval Diplomacy Perspective, Studies in Conflict & Terroris m, 47(212), pp. 1724-1746.

McNicholas, Michael A.Eds.(2016), Maritime Security An Introduction Second Editi on, Elsevier.

Ministry of Defense(2023), Defense of Japan 2023.

Ministry of Defense(2024), Defense of Japan 2024.

Ministry of Defense(2025), Defense of Japan 2025.

Østhangen, Andreas(2023), The Arctic after Russia's invasion of Ukraine: The incre ased risk of conflict and hybrid threats, Hybrid CoE.

Ringsberg, Anders Henrik, & Cole, Sebastian(2020), Maritime Security Guidelines: a Study of Swedish Ports' Perceived Barriers to Compliance, Maritime policy & Management, 47(3), pp 388-401.

Sari, Aurel(2025), Protecting Maritime Infrastructure from hybrid threats: legal opti ons, Hybrid CoE.

Eifuku, Seiya(2019), Maritime Security: Policies and Measures Seen in the Third Basi c Plan on Ocean Plicy and their Characteristics, etc., The national Institute for Defense Studies, NIDSコメンタリー, 81.

Stensrud, Cecilie Juul, & Østhangen, Andreas(2024), Hybrid warfare at Sea? Russia, Svalbard and the Arctic, Scandinavian Journal of Military Studies, 7(1), pp. 111-130.

US Government Accountability Office(2011), Report of Congressional Requesters, Coast Guard Security Risk Model Meets DHS Criteria, but More Training Cou ld Enhance its Use for Managing Programs and operations, US Government Accountability Office

United Nations General Assembly(2024), Resolution adopted by the General Assembly on 12 December 2024, Oceans and the law of the sea, A/RES/79/144.

United States Coast Guard(2016), National Search and Rescue Plan of the United States, US Department of Homeland Security.

UNODC(2013), Combating Transnational Organized Crime Committed at Sea.

UNODC(2019), Maritime Crime: a Manual for Criminal Justice Practitioners.

US Department of Homeland Security(2004.12.21.), National Security Presidential Directive –41 / Homeland Security Presidential Directive – 13 Maritime Security Policy, US Government.

법령정보

경찰청과 그 소속기관 직제(대통령령 제35970호, 2021.12.30.)

경찰청과 그 소속기관 직제 시행규칙(행정안전부령 제596호, 2025.12.30.)

관세법(법률 제20608호, 2024.12.31.)

관세법 시행령(대통령령 제35847호, 2025.12.30.)

국민보호와 공공안전을 위한 테러방지법(법률 제19580호, 2023.8.8.)

국제연합 초국가적 조직범죄 방지협약(조약 제2258호, 2015.12.5.)

국제항해선박 등에 대한 해적행위 피해예방에 관한 법률(법률 제18427호, 2021.8.17.)

국제항해선박 및 항만시설의 보안에 관한 법률(법률 제20125호, 2024.1.23.)

국제항해선박 및 항만시설의 보안에 관한 법률 시행규칙(해양수산부령 제750호, 2025.7.31.)

국제형사재판소에 관한 로마규정(조약 제1619호, 2003.1.30.)

남해지방해양경청과 그 소속기관 사무분장 규칙(남해지방해양경찰청훈령 제56호, 2025.7.1.)

대한민국 정부와 중화인민공화국 정부간의 어업에 관한 협정(제1567호, 2001.6.30.)

마약류 관리에 관한 법률(법률 제20878호, 2025.4.1.)(약칭: 마약류관리법)

밀항단속법(법률 제17006호, 2020.2.18.)

배타적 경제수역에서의 외국인어업 등에 대한 주권적 권리의 행사에 관한 법률(법률 제17616호, 2020.12.8.)(약칭: 경제수역어업주권법)

불법조업 외국어선 사법처리 절차 등에 관한 규칙(해양경찰청훈령 제139호, 2019.9.3.)

사이버안보 업무규정(대통령령 제34287호, 2024.3.5.)

선박 및 해상구조물에 대한 위해행위의 처벌 등에 관한 법률(법률 제17930호, 2021.3.16.)

어촌·어항법(법률 제17893호, 2021.1.12.)

영해 및 접속수역법(법률 제15429호, 2018.3.13.)

전기통신사업법(법률 제21065호, 2025.10.1.)

출입국관리법(법률 제20677호, 2025.1.21.)

폭력행위 등 처벌에 관한 법률(법률 제13718호, 2016.1.6.)

통합방위법(법률 제21065호, 2025.10.1.)

항만공사법(법률 제21065호, 2025.10.1.)

항만법(법률 제20231호, 2024.2.6.)

항만 출입절차에 관한 규정(해양수산부훈령 제737호, 2024.1.23.)

해사 사이버안전 관리지침(해양수산부고시 제2024-52호, 2024.5.9.)

해양경비법(법률 제18755호, 2022.1.11.)

해양경비법 시행규칙(해양수산부령 제581호, 2023.2.3.)

해양경찰청 사무분장규칙(해양경찰청훈령 제432호, 2025.5.14.)

해양법에 관한 국제연합 협약 및 1982년 12월 10일자 해양법에 관한 국제연합협약 제11부 이행에 관한 협정(다자조약, 제1328호, 1996.2.23.)

14 U.S.C.

Customs and Excise Management Act 1979(UK)

Illegal Migration Act 2023(UK)

Marine Navigation Act 2013(UK)

National Security Act 2023(UK)

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Acts of 2015, Public Law 114-23(USA)

海賊行為の処罰及び海賊行為への対処に関する法律(平成二十一年法律第五十五号, 令和4年6月17日)

인터넷 자료

1. 국내 자료

강원방송(2025.4.4.), 강원 무역항, 마약 안전지대 아니다, https://www.g1tv.co.kr/news/?mid=1_207_6&newsid=325982(검색일: 2025.4.25.)

경기신문(2025.3.12.), 인천해경, 중국에서 출항해 해상 밀입국 시도한 중국인 2명 검거, https://www.kgnews.co.kr/news/article.html?no=834835(검색일: 2025.4.24.)

경기신문(2024.5.2.), 해경청, 해상 밀항·밀입국 집중단속 나서, https://www.kgnews.co.kr/news/article.html?no=792216(검색일: 2025.4.24.)

경기일보(2024.11.11.), 해양경찰청, 김장철 맞아 김장 재료 밀수 행위 집중 단속나선다, https://www.kyeonggi.com/article/20241111580043(검색일: 2025.9.9.)

경기일보(2023.4.25.), 인천 내항서 밀입국 시도한 외국인…3시간 만에 검거, https://www.kyeonggi.com/article/20230425580236(검색일: 2025.3.10.)

경인일보(2023.11.7.), 중국서 '1조대 위조 명품' 밀수조직 입건, https://www.kyeongin.com/article/1663007(검색일: 2025.4.25.)

공공데이터포털(2025.3.18.), 해양경찰청 마약사범 단속현황(20241231), https://www.data.go.kr/data/15142026/fileData.do(검색일: 2025.4.28.)

국가물류통합정보센터, 선박입출항통계, https://www.nlic.go.kr/nlic/seaShipEtrypt.action(검색일: 2025.9.13.)

국가사이버안보센터, 국가사이버안보 수행체계, https://www.ncsc.go.kr:4018/PageLink.do(검색일: 2025.9.13.)

국가사이버안보센터, 사이버위협 대응, https://www.ncsc.go.kr:4018/PageLink.do(검색일: 2025.9.13.)

국가사이버안보센터(2024.9.2.), 정부 합동 '국가 사이버안보 기본계획' 발표, https://www.ncsc.go.kr:4018/main/PageLink.do(검색일: 2025.9.13.)

국가정보원, 국제범죄, https://www.nis.go.kr/AF/1_8.do(검색일: 2025.4.28.)

국가정보원, 사이버범죄, https://www.ncsl.or.kr/cybercrime(검색일: 2025.4.28.)

국가정보원, 사이버 테러리즘, https://www.ncsl.or.kr/cyberterrorism(검색일: 2025.4.28.)

나고야 항만청 홈페이지, https://www.port-of-nagoya.jp/english/authority/1001418.html(검색일: 2025.8.25.)

뉴스1(2024.2.9.), 마약 사범, 2.7만명 '역대 최다'…그 뒤엔 360만명 '신음'[일상된 마약①, https://www.news1.kr/society/general-society/5316407(검색일: 2025.4.28.)

대테러센터, 대테러체계, http://www.nctc.go.kr/nctc/activity/system.do(검색일: 2025.9.13.)

대한민국 정책브리핑(2025.7.14.), 법무부, '25년 1차 불법체류 외국인 정부합동단속 실시, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156698001(검색일: 2025.9.11.)

대한민국 정책브리핑(2024.10.31.), 해사사이버안전 관리 강화방안, https://www.korea.kr/briefing/policyBriefingView.do?newsId=156657855(검색일: 2025.9.7.)

대한민국 정책브리핑(2024.7.25.), 밀항·밀입국 등 해상 국경범죄 내달까지 단속 강화, https://www.korea.kr/news/policyNewsView.do?newsId=148931892(검색일: 2025.9.9.)

데일리안(2024.10.22.), 항만공사 등 해킹 시도, 5년간 1100건…국가 보안 '경보'[2024 국감], https://www.dailian.co.kr/news/view/1419796/(검색일: 2025.4.28.)

동아일보(2023.11.1.), "해상 밀입국, 국제 공조로 강력 대응", https://www.donga.com/news/Society/article/all/20231031/121962466/1(검색일: 2025.4.28.)

법무부((2024.12.19.), 법무부, '24년 2차 불법체류 외국인 정부합동단속 실시 약 1만 8천명 출국조치, https://www.moj.go.kr/bbs/moj/182/590443/artclView.do(검색일: 2025.9.11.)

서울뉴스(2023.7.17.), 또 찢어진 크램대교 폭발음... "14세 등 일가족 3명 사상"[포착], https://www.seoul.co.kr/news/international/2023/07/17/20230717500136(검색일: 2025.4.28.)

세계일보(2025.2.6.), 목포해경, 수개월 잠복 수사 끝에 외국인 마약사범 8명 검거, https://www.segye.com/newsView/20250206516568?OutUrl=naver(검색일: 2025.3.10.)

세계일보(2025.4.2.), 해경·관세청, 해상으로 마약류 대량 밀수 무역선 적발, https://www.segye.com/newsView/20250402518734(검색일: 2025.4.25.)

식품의약품안전처, 국내 마약류 관리, https://www.mfds.go.kr/wpge/m_1083/de010807l004.do(검색일: 2025.9.9.)

연안포털, 연안기본조사, https://coast.mof.go.kr/coastAdmin/research/socialNeconomy.do(검색일: 2025.4.28.)

연합뉴스(2025.10.6.), 태안 해상서 밀입국 시도 중국인 8명 검거…불법 취업 노려(종합), https://www.yna.co.kr/view/AKR20251006003251063(검색일: 2025.10.30.)

연합뉴스(2025.6.17.), 해군 지능정보화·유무인 복합체계 콘퍼런스 개최, https://www.yna.co.kr/view/AKR20250617034200504(검색일: 2025.9.6.)

연합뉴스(2025.4.15.), 진화하는 '해상 마약 밀수'... 단속 인력·장비는 제자리, https://www.ytn.co.kr/_cs/_ln_0115_202504150629373474_005.html(검색일: 2025.4.28.)

연합뉴스(2025.4.2.), 강릉 정박한 선박서 1조원어치 코카인 2t 적발 …'역대 최대'(종합2보), https://www.yna.co.kr/view/AKR20250402134852062(검색일: 2025.4.28.)

연합뉴스(2024.8.19.), 1천800억 코카인 밀반입…캐나다 마약 조직원 등 3명 구속(종합), https://www.yna.co.kr/view/AKR20240819042251065(검색일: 2025.4.28.)

연합뉴스(2024.1.26.), '영풍제지 주가조작' 주범 제주도서 밀항 시도하다 검거, https://www.yna.co.kr/view/AKR20240126088100004/(검색일: 2025.4.28.)

연합뉴스(2023.12.7.), [단독] 마약통로 된 '바닷길'…국내 유입 80% '선박 이용, https://www.yna.co.kr/view/MYH20231207022600641(검색일: 2025.4.28.)

연합뉴스(2023.4.9.), 적발하면 100만명분…해양 마약 5년 새 11배 '껑충', https://www.ytn.co.kr/_ln/0103_202304092255155890(검색일: 2025.4.28.)

연합뉴스(2022.9.15.), 국방과학연구소, 2022 민·군 해양무인자율체계 기술세미나 개최, https://www.yna.co.kr/view/PYH20220915172300013(검색일: 2025.9.6.)

연합뉴스(2019.9.16.), 드론 공격받은 사우디 아람코 석유시설, https://www.yna.co.kr/view/PYH20190916130400340(검색일: 2025.4.28.)

인천일보(2024.9.9.), 진화하는 마약 밀수법…단속 시스템 시급, https://www.incheonilbo.com/news/articleView.html?idxno=1265516(검색일: 2025.9.2.)

인천해양경찰서(2025.3.12.), 인천해경, 해상밀입국 시도한 외국인(2명) 검거, https://kcg.go.kr/inchoncgs/na/ntt/selectNttInfo.do?nttSn=59715(검색일: 2025.4.28.)

일요신문(2024.4.17.), 따개비 떼던 잠수부가 발견…화물선 역대급 마약 밀수 '기생충 수법' 뭐길래, https://www.ilyo.co.kr/?ac=article_view&entry_id=470738(검색일: 2025.3.10.)

외교부(2025.7.14.), 뉴포커스 2025 "세계신안보포럼" 준비를 위한 라운드테이블 개최, https://www.mofa.go.kr/www/brd/m_4076/view.do?seq=371494(검색일: 2025.9.6.)

외교부 보도자료(2025.9.8.),「2025 세계신안보포럼」개최결과. https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=376382(검색일: 2025.10.31.)

외교부 보도자료(2024.12.6.),「2024 세계신안보포럼」개최 결과, https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=375723&page=1&pitem=10(검색일: 2025.9.6.)

조선일보(2024.12.2.), 미사일 쏘는 최신형 러 공격 잠수함, 남중국해 나타났다… 무슨 일?, https://www.chosun.com/international/international_general/2024/12/02/MVBV2D5WXJGI7AAI7H7PSGNWCQ/(검색일: 2025.8.13.)

채널A뉴스(2025.1.20.), 부산 앞바다서 일본 밀입국 시도 중국인 일가족 검거, https://www.ichannela.com/news/main/news_detailPage.do?publishId=00000

0455871(검색일: 2025.3.10.)

천지일보(2023.7.26.), '해상 통해 무단이탈' 외국인 선원 2명 포착 검거, https://www.newscj.com/news/articleView.html?idxno=3048216(검색일: 2025.3.20.)

파이낸셜뉴스(2023.7.5.), 日나고야항 랜섬웨어 피해로 하역 못해 …경찰 수사 중, https://www.fnnews.com/news/202307051739447182(검색일: 2025.4.29.)

통계청, 관세청(관세행정정보시스템): 마약 밀수 검거 추이, https://www.index.go.kr/unity/potal/main/EachDtlPageDetail.do?idx_cd=1138(검색일: 2025.9.9.)

한겨레(2023.8.21.), 중국서 제트스키 300㎞ 타고 밀입국…군 포착 때까지 몰랐던 해경, https://www.hani.co.kr/arti/area/capital/1104976.html(검색일: 2025.3.10.)

한국어촌어항공단, 정주어항 현황(2022년 기준), https://www.fipa.or.kr/fipa/pgm/i-248/fixed/front/list.do(검색일: 2025.4.29.)

해사신문(2024.7.25.), "밀항·밀입국 범죄 절대 안돼"... 해양경찰, 단속 강화 나선다, http://www.haesanews.com/news/articleView.html?idxno=122172(검색일: 2025.9.9.)

해양경찰청(2025.2.6.), 2025년 주요업무 추진계획, https://www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?nttSn=59114(검색일: 2025.4.28.)

해양경찰청 보도자료(2025.9.3.), 해양경찰청, 미래 해양경비체계 발전을 위한 정책 공개토론회 개최, https://www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?nttSn=64212(검색일: 2025.9.7.)

해양경찰청 보도자료(2025.3.18.), 목포해경, 해·수산업 외국인 근로자 인권침해 점검, https://www.kcg.go.kr/mokpocgs/na/ntt/selectNttInfo.do?nttSn=59801(검색일: 2025.9.11.)

해양경찰청 보도자료(2025.2.17.), 「마약범죄 특별수사본부 제5차 회의」 개최, https://www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?mi=2799&nttSn=59215(검색일: 2025.9.9.)

해양경찰청 보도자료(2024.4.30.), 국가안보·어민 안전 위협하는 '외국어선 불법조업' 철퇴 -꽃게 성어기, 서해NLL 해역에서 불법 외국어선 단속에 총력, https://www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?nttSn=53217(검색일: 2025.9.6.)

해양경찰청 보도자료(2024.5.3.), 해경청, 해상 밀항·밀입국 집중단속 나서, https://

www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?nttSn=53333(검색일: 2025.9.9.)

해양경찰청 보도자료(2023.12.29.), 해양경찰청, 해양IT강국의 사이버수사 역량 제고, https://www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?nttSn=50407(검색일: 2025.9.13.)

해양경찰청 보도자료(2023.4.5.), 해양경찰청·관세청, 마약 단속을 위해 손을 맞잡다, https://www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?mi=2799&nttSn=44131(검색일: 2025.9.9.)

해양경찰청 보도자료(2021.7.19.), 해양경찰청, 하반기 국제범죄 집중 단속, https://www.kcg.go.kr/kcg/na/ntt/selectNttInfo.do?mi=2799&nttSn=31795(검색일: 2025.9.9.)

해양경찰청, 조직도, https://www.kcg.go.kr/kcg/cm/cntnts/cntntsView.do?mi=2825&cntntsId=63(검색일: 2025.9.13.)

해양수산부 보도자료(2025.6.23.), 높아지는 해사 사이버안전 관리의 중요성, 효과적 대응을 위해 한자리에 모인다, https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq=62054(검색일: 2025.9.7.)

해양수산부 보도자료(2025.5.1.), 제10차 OOC 성공리에 폐막, K-글로벌 해양 리더십 전 세계에 알려, https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq=61549(검색일: 2025.9.7.)

해양수산부 보도자료(2025.3.7.), 우리 국민, 바다에서도 안전하게! 민·관·군 해적대응 합동해상훈련 실시, https://www.mof.go.kr/doc/ko/selectDoc.do?docSeq=60805&listUpdtDt=2025-03-05++10%3A00&menuSeq=971&bbsSeq=10(검색일: 2025.9.11.)

해양수산부 보도자료(2024.10.31.), 선박 '사이버안전'으로 해상 물류 공급망 지킨다, https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq=59118(검색일: 2025.9.7.)

해양수산부 보도자료(2024.10.30.), 해적, 선박 테러 예방 정보를 한자리에, https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq=59079(검색일: 2025.9.7.)

해양수산부 보도자료(2023.11.28.), 선박 대테러 및 해적 대응 역량 높인다, https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq

=54115(검색일: 2025.9.7.)

해양수산부 보도자료(2023.4.21.), 해사 사이버안전 관리지침 제정, https://www.mof.go.kr/doc/ko/selectDoc.do?docSeq=50844&menuSeq=885&bbsSeq=35(검색일: 2025.9.13.)

해양수산부 보도자료(2022.11.28.), 선박 테러 및 해적행위, 이렇게 대비합니다, https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq=48006(검색일: 2025.9.7.)

해양수산부 보도자료(2022.11.24.), 스마트 해양시대의 사이버 위협, 어떻게 대응할까, https://www.mof.go.kr/doc/ko/selectDoc.do?menuSeq=971&bbsSeq=10&docSeq=47977(검색일: 2025.9.7.)

해양한국(2025.7.28.), 2025 해사 사이버안전 전문가 포럼, https://www.monthlymaritimekorea.com/news/articleView.html?idxno=54652(검색일: 2025.9.7.)

행정안전부 국가기록원(2017.12.26.), 북방한계선(NLL), https://www.archives.go.kr/next/newsearch/listSubjectDescription.do?id=010262&pageFlag=&sitePage=(검색일: 2025.8.31.)

현대해양(2024.11.14.), [해경, 항만공사 국감] 보안·안보 중요성 재각인 계기, https://www.hdhy.co.kr/news/articleView.html?idxno=30807(검색일: 2025.4.28.)

한국마약퇴치운동본부(2022), 마약류 현황 및 예방전략, 아름다운 젊음, 104, https://www.drugfree.or.kr/webzine/magazine/17/post-277.html(검색일: 2025.4.28.)

DiscoveryNews(2025.5.2.), 해양경찰청, 밀항·밀입국 등 해상 국경범죄 집중단속 추진, https://www.discoverynews.kr/news/articleView.html?idxno=1063461(검색일: 2025.9.9.)

해양안전종합정보시스템(GICOMS), 해적위험지수, https://www.gicoms.go.kr/pirate/selectPirateDangerList.do(검색일: 2025.9.11.)

kbc뉴스(2024.11.18.), '선착장에서 쓱'..마약 유통·투약 태국인 16명 덜미, https://news.ikbc.co.kr/article/view/kbc202411180073(검색일: 2025.3.10.)

KBS뉴스(2024.6.20.), 부산신항 입항 화물선에서 코카인 33㎏ 발견…'배달사고' 추정, https://news.kbs.co.kr/news/pc/view/view.do?ncd=7992350(검색일:

2025.4.28.)

KBS뉴스(2024.1.16.), 부산항 화물선 바닥서 코카인 의심 물질 100kg 발견, https://news.kbs.co.kr/news/pc/view/view.do?ncd=7867360(검색일: 2025.4.28.)

Korea Shipping Gazette(2024.12.31.), 특별기고/차세대 선박의 변화와 대응, https://www.ksg.co.kr/news/main_newsView.jsp?pNum=143461(검색일: 2025.9.6.)

MBC뉴스(2024.1.5.), 후티 반군, 홍해에서 무인수상정 동원해 공격, https://imnews.imbc.com/news/2024/world/article/6559625_36445.html(검색일: 2025.4.28.)

YTN(2021.5.24.), AI 감시에도 또 뚫린 인천항…베트남 선원 밀입국, https://www.ytn.co.kr/_ln/0103_202105240456121941(검색일: 2025.3.10.)

YTN(2021.10.24.), 한-중 해저 케이블 일부 끊어져…일부 통신 '먹통', https://www.ytn.co.kr/_ln/0104_202110241404417156(검색일: 2025.4.29.)

2. 국외 자료

AP NEWS(2025.6.3.), A surprise drone attack on airfields across Russia encapsulates Ukraine's wartime strategy, https://apnews.com/article/what-to-know-ukraine-drone-attack-russia-bombers-2d01b23341e2289882760b9f121431d4(검색일: 2025.7.17.)

AP NEWS(2025.1.28.), At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard, https://apnews.com/article/nato-france-russia-baltic-cables-ships-damage-764964a275530915c2cc5af1125ec125(검색일: 2025.7.17.)

Business Insider(2025.5.4.), Ukraine said it downed fighter jets with drone boats for the 'first time in history,' destroying two $50 million Russian aircraft(검색일: 2025.7.17.)

CNBC(2017.8.16.), Shipping company Maersk says June cyberattack could cost it up to $300 million, https://www.cnbc.com/2017/08/16/maersk-says-not petya-cyberattack-could-cost-300-million.html(검색일: 2025.4.28.)

CSIS(2019.8.5.), Irans' Threat to Saudi Critical Infrastructure: The Implications of

US-Iranian Escalation, https://www.csis.org/analysis/irans-threat-saudi-critical-infrastructure-implications-us-iranian-escalation#:~:text=The%20Houthis%20have%20used%20these,missile%20parts%20to%20the%20Houthis.(검색일: 2025.9.2.)

CSIS(2025), Significant Cyber Incidents since 2006, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents(검색일: 2025.9.2.)

CSIS(2021.12.21.), The Iranian and Houthi War against Saudi Arabia, https://www.csis.org/analysis/iranian-and-houthi-war-against-saudi-arabia(검색일: 2025.9.2.)

DEA Museum, DEA on the Sea, https://museum.dea.gov/exhibits/online-exhibits/dea-air-land-and-sea/dea-sea(검색일: 2025.8.14.)

Department of Homeland Security, Global Maritime Operational Threat Response (MOTR) Coordination Center (GMCC), https://www.dhs.gov/global-motr-coordination-center-gmcc(검색일: 2025.8.14.)

Department of Homeland Security, Creation of the Department of Homeland Security, https://www.dhs.gov/creation-department-homeland-security (검색일: 2026.1.19.)

DNV, Marine fleet management software and ship management systems-ShipManager, https://www.dnv.com/services/marine-fleet-management-software-and-ship-management-systems-shipmanager-114260/(검색일: 2025.7.17.)

DP World, DP World Australia Overview, https://www.dpworld.com/en/about-us/our-locations/australia(검색일: 2025.7.17.)

DW(2023.9.25.), Politics Europe, Nord Stream pipelines blasts: A maze of speculation, https://www.dw.com/en/nord-stream-pipelines-blasts-a-maze-of-speculation/a-66913853(검색일: 2025.4.28.)

European Commission(2016), Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018(검색일: 2025.4.28.)

FBI(2002.8.5.), Testimony, https://archives.fbi.gov/archives/news/testimony/homeland-security-facilitating-and-securing-seaports(검색일: 2025.8.14.)

FBI(2025.12.11.), News Worldwide Threats too the Homeland, https://www.fbi.gov/news/speeches-and-testimony/worldwide-threats-to-the-homeland-121125(검색일: 2025.12.11.)

Foreign Policy(2024.12.4.), The Baltic Sea's Bad Actors, Russian and Chinese gray-zone aggression prove that dreams of a peaceful "NATO lake" were prematrue, https://foreignpolicy.com/2024/12/04/russia-china-baltic-sea-nato-subsea-cables-ais-spoofing/(검색일: 2025.4.28.)

HMCG, What we do, https://hmcoastguard.uk/what-we-do(검색일: 2025.4.25.)

Hybrid CoE, Dates of accession for the Hybrid CoE Participating States, https://www.hybridcoe.fi/wp-content/uploads/2024/08/Hybrid_CoE_Participating-states_Albania_240830.pdf(검색일: 2025.4.28.)

Hybrid CoE, Establishment, https://www.hybridcoe.fi/establishment/(검색일: 2025.4.28.)

Hybrid CoE, Hybrid threats as a concepts, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/(검색일: 2025.4.28.)

Hybrid CoE, What is Hybrid CoE, https://www.hybridcoe.fi/who-what-and-how/(검색일: 2025.4.28.)

IMO, Maritime Safety Committee - 108th session(MSC 108), 15-24 May 2024, https://www.imo.org/en/mediacentre/meetingsummaries/pages/msc-108th-session.aspx(검색일: 2025.8.25.)

JMSC, Joint Maritime Security Centre, https://www.gov.uk/government/groups/joint-maritime-security-centre(검색일: 2025.4.25.)

MCA, About us, https://www.gov.uk/government/organisations/maritime-and-coastguard-agency/about#corporate-information(검색일: 2025.4.25.)

Naval Technology(2025.6.11.), UK Distl tests underwater robot to clear unexploded ordnance, https://www.naval-technology.com/news/uk-dstl-tests-underwater-robot/?cf-view(검색일: 2025.7.17.)

Penta Security(2025.6.11.), サイバーセキュリティ基本法とは？法改正の要点 · 企

業が取るべき対策を含めて解説, https://www.pentasecurity.co.jp/pentapro/entry/basic-act-cybersecurity(검색일: 2025.8.15.)

Popular mechanics(2016.3.2.), Sea Pirates Hacked a Shipping Company To Figure Out Which Vessels to Plunder, https://www.popularmechanics.com/technology/infrastructure/a19719/sea-pirates-hacked-a-shipping-firm/(검색일: 2025.4.30.)

Port of Seattle(2024.9.13.), Port Cyberattack Archive, https://www.portseattle.org/news/port-cyberattack-archive(검색일: 2025.4.29.)

Reuters(2025.2.22.), Recent suspected underwater sabotage incidents in the Baltic Sea, https://www.reuters.com/world/europe/recent-suspected-underwater-sabotage-incidents-baltic-sea-2024-12-03/(검색일: 2025.4.28.)

Reuters(2024.12.4.), As sabotage allegations swirl, NATO struggles to secure Baltic Sea, https://www.reuters.com/world/sabotage-allegations-swirl-nato-struggles-secure-baltic-sea-2024-12-03/(검색일: 2025.7.17.)

Snow Eagle Group, Maritime Security Risk Analysis Model(MSRAM), https://www.snoweaglegroup.com/portfolio/maritime-security-risk-analysis-model-msram/(검색일: 2025.9.13.)

Talarian, Geocode by Awesome Table, https://workspace.google.com/marketplace/app/geocode_by_awesome_table/904124517349(검색일: 2025.9.13.)

The Record(2023.1.17.), Ransomware attack on maritime software impacts 1,000 ships, https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships(검색일: 2025.4.30.)

TWZ(2025.6.12.), Houthi Drone Boat Strikes Ship For First Time Since Red Sea Crisis Erupted, https://www.twz.com/news-features/houthi-drone-boat-strikes-ship-for-first-time-since-red-sea-crisis-erupted(검색일: 2025.7.17.)

TXOne Networks(2024.1.22.), Future Cybersecurity Threats in Ports: Protecting Global Trade from Rising Maritime Risks, https://www.txone.com/blog/protecting-global-trade-from-rising-maritime-risks/(검색일: 2025.4.29.)

UK Government(2022.8.15.), Policy Paper, National Maritime Security Strategy, https://www.gov.uk/government/publications/national-maritime-security-strategy(검색일: 2025.10.7.)

U.S. Central Command(2025.6.12.), June 12 U.S. Central Command Update, https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/3805237/june-12-us-central-command-update/(검색일: 2025.7.17.)

U.S. Customs and Border Protection, Customs Trade Partnership Against Terrorism (CTPAT), https://www.cbp.gov/border-security/ports-entry/cargo-security/CTPAT(검색일: 2025.8.14.)

U.S. Customs and Border Protection, CSI: Container Security Initiative, https://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief(검색일: 2025.8.14.)

U.S. Department of Justice, Our Work, https://www.justice.gov/our-work(검색일: 2025.8.14.)

U.S. Immigration and Custoomos Enforcement(2025.5.28.), https://www.ice.gov/news/releases/ice-federal-partners-conduct-immigration-enforcement-operations-nantucket-marthas(검색일: 2025.8.14.)

United States Coast Guard, ISPS/MTSA, https://www.dco.uscg.mil/ISPS-MTSA/(검색일: 2025.8.14.)

United States Coast Guard News(2025.7.16.), Final Rule: Cybersecurity in the Marine Transportation System – Implementation Timeline, https://www.news.uscg.mil/maritime-commons/Article/4247529/final-rule-cybersecurity-in-the-marine-transportation-system-implementation-tim/(검색일: 2025.8.13.)

United States Coast Guard News(2025.1.17.), Final Rule: Cybersecurity in the Marine Transportation System, https://www.news.uscg.mil/maritime-commons/Article/4033732/final-rule-cybersecurity-in-the-marine-transportation-system/(검색일: 2025.8.18.)

영국 법령 포털, https://www.legislation.gov.uk/primary+secondary?title=Marine%20Navigation%20Act%202013(검색일: 2025.8.14.)

영국 법령 포털, https://www.legislation.gov.uk/ukpga/1979/2/contents(검색일: 2025.8.15.)

영국 법령 포털, https://www.gov.uk/government/collections/illegal-migration-bill(검색일: 2025.8.16.)

영국 정부, Cyber Security and Resilience Bill, https://www.gov.uk/government/collections/cyber-security-and-resilience-bill(검색일: 2025.8.15.)

영국 정부, Departmenf for Transport, https://www.gov.uk/government/organisations/department-for-transport/about(검색일: 2025.4.28.)

영국 정부, Impact assessment, Border Security, Asylum and Immigration Bill 2025: overarching impact assessment(accessible), https://www.gov.uk/government/publications/border-security-asylum-and-immigration-bill-2025-impact-assessment/border-security-asylum-and-immigration-bill-2025-impact-assessment-accessible(검색일: 2025.8.15.)

영국 정부, Maritime and Coastguard Agency, https://www.gov.uk/government/organisations/maritime-and-coastguard-agency/about(검색일: 2025.4.29.)

영국 정부, National Security Act Factsheet, https://homeofficemedia.blog.gov.uk/2023/07/11/national-security-act-factsheet/(검색일: 2025.8.15.)

일본대백과전서, テロ等準備罪, https://japanknowledge.com/contents/nipponica/sample_koumoku.html?entryid=807(검색일: 2025.8.14.)

일본 법무성, テロ等準備罪について, https://www.moj.go.jp/keiji1/keiji12_00143.html(검색일: 2025.8.14.)

일본 법무성, https://laws.e-gov.go.jp/law/329AC0000000061(검색일: 2025.8.14.)

일본 법무성, https://laws.e-gov.go.jp/law/326CO0000000319(검색일: 2025.8.14.)

일본 세관, Organization of Regional Customs, https://www.customs.go.jp/english/zeikan/z-kikou_e.htm(검색일: 2025.8.14.)

일본 출입국재류관리청, 出入国在留管理庁の概要, https://www.moj.go.jp/isa/(검색일: 2025.8.14.)

일본 해양종합정책본부, 内閣官房: 総合海洋政策本部, https://www.kantei.go.jp/jp/singi/kaiyou/index.html(검색일: 2025.8.14.)

코넬대 로스쿨 법령정보센터, U.S. Code: Table Of Contents, https://www.law.cornell.edu/uscode/text(검색일: 2025.8.13.)

부 록

1. 주요 선행연구 현황

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
1	• 연구명: 항만보안 관할권 소재에 관한 법적 고찰 • 연구자(연도): 함혜현·전봉조·이장욱(2022) • 연구 목적: 해상국역에 대한 보안관할권 범위를 분석하여 관할권 개선을 위한 입법적 개선책 제시	• 문헌연구 • 관련 제도 및 정책 분석 • 전문가 자문	• 항만보안의 개념, 항만보안 관할권의 개념, 법적 성격 분석 • 항만보안 체계의 구조적 특성에 따른 관할 사각지대 분석 • 항만보안 관할권 관련 기관의 소관 법령 등 권한 범위 분석 • 항만보안사고의 예방과 대응을 위한 입법적 개선방안 제시
2	• 연구명: 해양의 안전관리를 위한 법제 개선방안 연구 • 연구자(연도): 이순태·이유봉(2017) • 연구 목적: 해양에서 발생하는 위험에 대한 분석과 이에 대한 대응정책, 대응기관, 집행작용, 관련 법령 분석을 통해 위험을 보다 적절히 관리할 수 있는 방안 모색	• 문헌연구 • 통계분석 • 소셜 빅데이터 분석 • 비교 정책 및 법령 분석	• 해양안전과 해양안보의 개념과 범위 • 해양 안전관리에 관한 빅데이터 분석 • 해양 안전관리에 관한 주요 법령 체계 분석 • 해양 안전관리에 관한 국제법 및 비교법적 분석 • 입법개선을 위한 정책 제언
3	• 연구명: 해양 선박재난 대응을 위한 거버넌스 법제 연구 • 연구자(연도): 방호삼·하민재(2022) • 연구 목적: 재난 및 안전관리 기	• 문헌연구 • 국별 정책 및 법령 비교 분석	• 주요 국가의 해양 선박재난 대응체제 비교 • 해양 선박재난 대응체계 분석 • 해양 선박재난 대응 주관기관 역할 분석

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
	본법을 근거로 해양사고 주관기관과 현장대응기관과의 역할 분석 및 제도 개선 사항 제시		• 해양 선박재난 대응 거버넌스 법제 입법 방안
4	• 연구명: 자율운항선박의 기술동향과 법정책 이슈 • 연구자(연도): 김희정(2022) • 연구 목적: 자율운항선박 관련 국내외 기술 발전에 따른 법정책 동향과 함께 자율운항선박의 자율 시스템 단계별 이슈, 안정성 이슈, 사고 책임 이슈 등에 관한 법정책 이슈를 통해 시사점을 도출	• 문헌연구 • 기술동향 분석 • 국별 정책 및 법령 비교 분석	• 자율운항선박 분야의 환경변화 • 자율운항선박의 개념과 기술 동향 • 국제기구 및 글로벌 자율운항선박 법정책 동향 • 국내 자율운항선박 법정책 개발 현황 • 자율운항선박 관련 선박성, 개발 단계별 법적 이슈, 안전성 이슈, 사고 책임 이슈, 제조물 책임 이슈, 보안 이슈 분석
5	• 연구명: 마약류 등 유해약물의 사회적 비용 분석 • 연구자(연도): 박성수(2018) • 연구 목적: 2016년 기준 마약류 등 유해약물로 인한 사회적 비용을 추계	• 문헌연구 • 기초통계분석 • 비용편익분석 • 조건부 가치측정법 • 인적자원접근법, 간접비용 추계 등	• 마약류 등 유해약물의 사회적 비용의 이론적 논의 • 마약류 등 유해약물의 사회적 비용 분석 • 마약류 등 유해약물의 의의 및 실태 • 마약류 등 유해약물의 사회적 비용 분석 방법론
6	• 연구명: 해양경찰의 정보활동 실태 및 발전 방안 연구 • 연구자(연도): 문경환(2017) • 연구 목적: 해양경찰의 정보조직 체계 및 활동 범주에 대해 살펴보고 정보관을 대상으로 한 심층 인터뷰 결과를 토대로 해양경찰의 정보활동 방향과 정보교육·훈련에 대한 발전방안을 제시	• 문헌연구 • 통계분석 • 전문가 자문 및 인터뷰 • 일본 정책 동향 비교 분석	• 해양경찰 정보조직 및 활동 범주 분석 • 해양경찰의 정보교육 및 훈련 현황 • 해양정보경찰활동 및 교육, 훈련에 대한 인식 분석
7	• 연구명: 항만보안 관리체계 효율화 방안 연구 • 연구자(연도): 김찬호·최건우·박상원(2017) • 연구 목적: 2016년 기준 마약류	• 문헌연구 • 통계분석 • 국별 정책 및 법령 비교 분석	• 항만시설보안료 징수관련 현황 및 문제점 • 항만보안 관리, 감독 관련 현황 및 문제점 • 국내외 교통분야 관리 감독 체계 분

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
	등 유해약물로 인한 사회적 비용을 추계		석 • 항만보안 관리체계 효율화 방안 제시
8	• 연구명: 항만 등 국가중요시설 민간경비체계의 법적 문제와 개선방안 • 연구자(연도): 김재광(2019) • 연구 목적: 항만 등 국가중요시설에 대한 민간경비체계의 법적 과제를 경비 및 경찰의 관점에서 분석하고 그에 대한 개선방안을 제시	• 문헌연구 • 기초통계분석 • 국내외 제도 분석	• 항만 등 국가중요시설의 위험방지의 법적 함의 • 항만 등 국가중요시설 민간경비 체계의 법적 문제 • 항만 등 국가중요시설 민간경비 체계의 법적 개선방안
9	• 연구명: 한국형 해양상황인식체계 구축을 위한 시스템간 표준화 연계방안에 관한 연구 • 연구자(연도): 김영습 외(2021) • 연구 목적: 해양상황의 인식을 위해 현재 해양경찰청에서 운영중인 시스템(Radar, VHF, V-Pass 등)별 정보 현황을 분석하고 이들 시스템 간의 정보연계를 위한 데이터 및 통신 표준안과 관련 규정의 적용 방안을 제시	• 문헌연구 • 기초통계분석 • 공동(집단작업) 연구	• 감시자산을 통해서 미식별 선박 및 불온선박 등을 탐지하기 위한 이기종 간 감시자산 연계 방안을 제시 • 해양경찰 감시자산 시스템 운영현황 및 문제점 • 해양경찰 감시자산 장비별(Radar, VHF, AIS, V-Pass 등) 통신표준 내용 • 감시자산 장비별 정보연계를 위한 표준화 방안
10	• 연구명: 한국의 해양영역인식에 관한 연구-해양영역의 변화를 중심으로- • 연구자(연도): 백병선(2018) • 연구 목적: 한국의 해양영역에 대한 인식 변화를 분석하고, 이를 바탕으로 안보, 안전, 경제, 환경, 협력 등 다섯 가지 영역을 중심으로 한국의 해양영역인식에 대한 개념을 정립	• 문헌연구 • 기초통계분석 • 비교 정책 분석 • 사례 분석	• 해양영역에 대한 접근(자유로운 접근과 지배적 접근) • MDA에 대한 인식 변화와 안보, 국부, 협력의 관점에서 해양영역의 분류 • 해군 및 해양경찰의 해양영역에 대한 인식과 중앙부처 및 지자체의 해양영역 인식 변화 • 우리나라 해양영역의 영역별(안보, 안전, 경제, 환경, 협력) 위협 요소 및 대응방안 도출
11	• 연구명: 인도·태평양 지역 '해양상황인지' 현황과 '쿼드(Quad)' 국가의 기여: 쟁점 및 전망	• 문헌연구 • 기초통계분	• MDA 개념과 정보의 수집·융합·공유

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
	• 연구자(연도): 이정훈 외(2020) • 연구 목적: 쿼드 국가가 인·태 지역 해양상황인지(MDA) 능력 배양을 위한 소다자 협력의 플랫폼으로서 쿼드 협력체 활용에 대해 분석, 이를 통한 시사점 도출	석 • 비교 정책 분석 • 사례 분석	• 인·태 지역 MDA 현황과 쟁점 • 인·태 지역 MDA 능력배양을 위한 쿼드 국가의 개별적 기여와 중국의 대응 • 인·태 지역 MDA 능력배양을 위한 쿼드 국가 간 협력과 외연 확장
12	• 연구명: 한국형 해양상황인식(MDA) 체계 – 구축 방안 연구를 중심으로 • 연구자(연도): 장윤석(2022) • 연구 목적: 국내·외 감시자산 현황과 발전 동향 등을 분석하여 한국형 MDA 구축을 위한 방안 등을 제시	• 문헌연구 • 기초통계분석 • 비교 정책 분석	• 해양 정보 수집 및 분석에 관한 국제 해양정세 분석 • 미국 및 일본의 MDA 구축 실태조사 및 분석 • 한국형 MDA 구축을 위한 요건 및 구축 방안
13	• 연구명: 특별수사기관의 수사체계 안착방안 연구(II) – 해양경찰을 중심으로 • 연구자(연도): 박경규 외(2023) • 연구 목적: 2022년 검경 수사권 조정 이후 특별수사기관인 해양경찰의 수사체계를 분석하여 해양환경특수성을 반영한 개선 및 수사역량 강화방안에 대해 살펴보는 것을 목적으로 함	• 문헌연구 • 기초통계분석 • 비교 정책 분석	• 해양경찰 수사체계 및 관할 범위 등을 분석 • 해양경찰 수사관할 범죄인 해양범죄 유형과 현황을 분석 • 미국 USCG, 독일 해상경찰조직, 영국 MCA, 일본 해상보안청 등의 수사체계를 검토 • 해양경찰 수사체계 개선 사항으로 인적자원, 해양경비법상의 해상검문검색권의 개선, 개별 범죄군에 대한 개선 사항 제언
14	• 연구명: 해양범죄의 수사역량 강화를 위한 해양경찰 수사교육전문화에 관한 연구 • 연구자(연도): 김재운(2014) • 연구 목적: 해양범죄의 일반적 수사관할을 가지는 해양경찰의 범죄수사전문가 양성을 위한 전문교육기관 설치 필요성을 연구	• 문헌연구 • 관련 정책 및 법 분석 • 비교 정책 분석	• 해양범죄를 유형별로 구분하고 이에 대한 특징과 발생 실태를 분석 • 해양경찰 수사교육 실태와 문제점 분석을 위해 국내 해양경찰 수사요원 교육과정, 외국 해양안전기관의 수사교육을 비교하여 분석 • 해양범죄 수사교육 기회의 부족, 해양범죄 전문수사과정 개발의 부족 등의 문제를 개선하기 위해 전문교수요원 양성, 관련 정보의 축적, 전문교육과정 및 교육기관의 설치 등을 제시

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
15	• 연구명: 해양 밀입국 실태와 해양경찰의 대응방안 • 연구자(연도): 유재두·노호래(2018) • 연구 목적: 해상밀입국이 경제적 이유에서 사회·문화적 이유로 확대되고, 그 방법 또한 신분 위장 등 고도화되고 있어 이에 대응하기 위한 대책을 연구 및 제시	• 문헌연구 • 통계분석 • 관련 정책 및 법 분석 • 사례연구	• 해양 밀입국 개념 및 법적 근거를 분석하고 해양 밀입국의 원인과 특성을 분석 • 해양 밀입국 실태 분석을 위해 1994년 발생했던 중국 조선족 밀입국 사례 등을 분석 • 밀입국 단속 통계를 분석하여 해양 밀입국 유형을 분석하고 문제점 도출 • 개선방안으로 해양밀입국 단속 강화(항만 CCTV 확충 등), 국제공조 강화, 공간 분석 등을 제시
16	• 연구명: KANO 모델을 활용한 연안 지역의 CPTED 수요 분석 • 연구자(연도): 정아신·양쥔·조정형(2024) • 연구 목적: 많은 유동 인구로 범죄 발생 확률이 높은 연안지역 부산 미포마을을 대상으로 KANO 모델을 활용한 범죄예방환경디자인(CPTED)을 적용한 범죄율 감소 방안을 제시	• 문헌연구 • 통계분석 • KANO 모델 기반 CPTED • 현장 조사	• CPTED를 위한 KANO 모델에 관한 이론적 분석 • 부산 미포마을의 KANO 모델을 적용한 CPTED 수요도 조사 • KANO 모델 CPTED 수요도 조사 결과에 따라 미포마을의 경우, 순서대로 자동 경보 장치/지역 특성에 부합한 디자인 스타일/각 기능 구역 공간 분할/CCTV/가로등(조명시설) 설치/환경 색깔 통일/차량 분류/LED 스마트 스크린/디자인 스타일 간결함/안전표시/비상 통화 버튼 등이 우선적으로 중요한 환경임을 제시
17	• 연구명: 연안여객선의 보안위협 대응방안에 관한 연구 • 연구자(연도): 주종광·이은방(2007) • 연구 목적: 연안여객선 보안위협과 관리제도 현황을 분석하고 관련 종사자들에 대한 보안의식을 설문조사하여 분석함으로써 연안여객선의 보안취약성과 보안위협의 특성을 도출	• 문헌연구 • 설문조사 • 관련 정책 및 법 분석	• 연안여객선 보안위협 수준을 이용자 및 선박 운항 현황을 기준으로 분석 • 연안여객선의 잠재적인 보안 위협을 일곱 가지로 분류하고 이에 대한 보안위험관리 현황을 분석 • 보안의식을 조사 및 분석하기 위해 연안여객선 선박직원, 운항관리자, 해양경찰, 여객을 대상으로 설문조사를 실시하여 연안여객선 보안 취약성을 분석 • 여객선 보안 문화 개선을 위해 연안여객선 보안제도 수립, 보안장비 개

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
			발, 보안시스템 구축 등을 제시
18	• 연구명: 해양경찰 정보활동의 법적 근거와 범위에 관한 고찰 • 연구자(연도): 최정호(2016) • 연구 목적: 해양경찰의 정보기능이 내실 있게 수행되기 위해 법적 보완 사항, 해양경찰 정보활동 특화 분야 개발, 바다와 관련된 각종 정보를 다루는 관련 기관과의 연계 등을 제시	• 문헌연구 • 관련 정책 및 법 분석 • 전문가 자문	• 해상정보활동의 개념, 범위를 이론적으로 검토하고, 해양경찰 정보활동의 실태를 조직관점에서 검토 • 해상정보활동의 법적 근거를 정부조직법, 경찰관 직무집행법, 경찰법 등을 중심으로 검토하고 이를 통해 치안정보 활동의 법규성을 확인 • 또한 정책 및 직무를 수행하는 데 필요한 정보 및 자료 수집 활동을 해양경찰청의 권한 내에서 시행할 수 있음을 분석 • 다만, 적절한 정보활동을 위한 조직의 현실화, 해양수산 분야 정책정보 수집, 제도보완, 해양 정보활동 특화 분야 활성화 등을 제도 개선사항으로 제시
19	• 연구명: 한국 해양경찰청과 일본 해상보안청의 국제해양범죄수사기능 비교 및 시사점 • 연구자(연도): 한재진·최정호(2020) • 연구 목적: 해양경찰청과 일본 해상보안청의 일반범죄 및 국제해양범죄 수사현황을 비교하여 분석하고 우리나라 해양경찰청의 국제범죄수사기능의 발전 및 개선 방향을 제시	• 문헌연구 • 기초통계분석 • 관련 정책 및 법 분석 • 비교 정책 분석 • 사례 분석	• 한국과 일본의 해양범죄에 관한 법적 개념을 비교 분석하고, 관련 범죄통계를 분석하여 각국 해양범죄의 경향성과 특징을 분석 • 한국과 일본의 해양범죄 수사기관의 조직구조, 수사인원, 보유 자원(함정 등)을 분석 • 특히 국제형사(외사)조직의 특징을 분석하여 비교하여 일본 조직의 전문성과 특수성을 시사점으로 도출 • 해양경찰청 국제범죄수사 개선 방향으로 외사의 국제범죄수사기능을 체계화하고 전문인력을 양성하며, 정보 수집 역량 제고와 국제공조 활성화 등을 제시
20	• 연구명: 해양 대테러 정보활동 발전방안 연구 • 연구자(연도): 함혜현(2022) • 연구 목적: 해양테러 주관기관인 해양경찰청의 정보 수집 권한 확보를 위한 발전방안을 제시	• 문헌연구 • 관련 정책 및 법 분석 • 비교 정책 분석 • 사례 분석	• 해양 대테러 정보활동의 개념 및 법적 근거를 도출하기 위해 「테러방지법」 등의 관련 법·제도를 분석 • 주요 선진국(미국, 캐나다, 일본)의 해양 대테러 기관의 정보활동을 분석하여 인간정보, 기술정보 수집 등

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
			에 관한 법적 권한 부여에 관한 사실을 비교 분석 • 해양 대테러 정보활동 발전방안으로 정보 수집 역량 강화방안, 유관기관 협력 강화, 해양경찰청 내 정보 공유 체계 수립 등을 제시
21	• 연구명: Preventing Catastrophic Cyber-Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore • 연구자(연도): Fenton(2024) • 연구 목적: 말라카 해협과 싱가포르 해협의 복합위협을 검토하고, 특히 사이버 등을 통한 위협을 대비하기 위한 해협 인접 국가들의 협력 방안을 제시	• 문헌연구 • 설문조사 • 시뮬레이션 • 관련 정책 분석	• 선박 운항의 핵심 시스템이 IT 기술 등을 통해 상호 연결성이 확장되고 있지만, 선원 및 관련자들의 사이버 보안 인식 부족 • 특히 이슬람 근본주의 및 폭력주의자들이 온라인 도구를 통한 사이버 위협이 증가 • IMO는 사이버 보안 등에 관한 지침은 구체성이 부족하여 위협을 실제로 대응하기 미흡 • 이에 말라카 및 싱가포르 해협에서 사이버를 통한 선박 연쇄 충돌 및 테러사고 발생가능성이 시뮬레이션 등을 통해 검증 • 위협완화 및 예방 방안으로 인접국가들의 사이버 공격 보고 시스템 구축, 선상 훈련 체계 강화, 지역 협력 등을 제시
22	• 연구명: Maritime Security Guidelines: a study of Swedish ports' perceived barriers to compliance • 연구자(연도): Ringsberg & Cole(2020) • 연구 목적: 해상교통에 대한 해적 및 테러 위협의 증가를 극복하기 위한 유럽해양보안지침(MSGs)의 스웨덴 국내 도입 방안을 제시	• 문헌연구 • 설문조사 • 전문가 자문 • 관련 정책 분석	• 유럽해양보안지침 도입 장벽을 분석하기 위한 방법론 개발 • 유럽해양보안지침 도입 장벽을 분석하기 위해 전문가 자문 및 설문조사를 실시 • 이를 통해 도입 장벽으로 스웨덴 해양보안 관계기관의 협력, 이용가능한 자원의 부족, 보안 문화 및 지식 부족, 지침의 구체적인 운용 방안 부재 등을 도출 • 이에 관련 기관 해양보안교육 활성화를 통한 네트워크 강화, 소규모 항만에 지침 적용을 위한 관련 국제 표준의 활용 등을 방안을 제시

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
23	• 연구명: National and international maritime situational awareness model examples and the effects of North Stream Pipelines sabotage • 연구자(연도): Gülcan & Erginer(2023) • 연구 목적: 새로운 위협과 리스크를 중심으로 해양영역인식(MDA) 또는 해양활동인식(MSA)으로 일컬어지는 해양전략을 분석하여 노르트스트림 가스 관선에 대한 영향을 도출	• 문헌연구 • 통계분석 • 비교 정책 분석 • 사례연구	• 해양안전 및 안보의 개념을 분석하고 해양상황인식(MSA)과 해양영역인식(MDA)에서 고려되어야 할 요소를 구분하여 제시 • EU, 미국, 영국, 호주, 싱가포르, 인도, 남아프리카공화국의 MSA와 MDA를 위한 정보체계를 개괄하고 관련 부처의 기능 분석 • 해양안보측면에서 노르트스트림 가스 관선 운영 중단의 영향을 분석하고 MSA로서 대처방안 제시
24	• 연구명: Crimes committed at Sea and criminal jurisdiction • 연구자(연도): Fabris(2017) • 연구 목적: 해양범죄의 국가관할권에 관한 국제법을 분석하고 관할권 적용에 있어서 국가 간 차이점을 분석(엔리카렉시호 사건)	• 문헌연구 • 관련 국제법 및 정책 분석 • 판례 분석	• 엔리카렉시호 사건 원인 및 상황 분석 • 해양범죄에 대한 국가관할권을 분석 • 유엔해양법협약상 해양범죄의 관할권 • 해상테러 및 해적에 대한 관할권의 특별규칙 • 엔리카렉시호에 있어서 관할권 적용
25	• 연구명: Combating Transnational Organized Crime Committed at Sea • 연구자(연도): UNODC(2013) • 연구 목적: UN 마약 및 범죄 사무소에서 해상에서 발생하는 조직범죄 중 해적, 해상강도, 인신매매, 마약 밀수, 불법조업 범죄 등에 대한 문제점을 분석하고 이에 대한 정책적 대응 방안을 제시	• 문헌연구 • 관련 국제법 및 정책 분석 • 현장조사 • 사례소개 • 전문가 자문	• 해상에서의 국제조직 범죄 개요 소개 • 해적과 해상강도 법적 근거와 문제점 • 해상의 밀입국과 인신매매의 법적 근거와 문제점 • 마약 밀수에 관한 법적 근거와 문제점 • 불법조업 등 수산범죄의 법적 근거와 문제점
26	• 연구명: Maritime Crime: a Manual for Criminal Justice Practitioners	• 문헌연구 • 관련 국제법 및 정책 분석	• 해상범죄에 적용되는 법률 • 해양수역의 구분과 수역별 국가의 권한 해상에서 법집행

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
	• 연구자(연도): UNODC(2019) • 연구 목적: UN 마약 및 범죄 사무소에서 개발한 해상범죄 단속 및 법집행에 관한 국제법적 근거 및 실무 지침	• 사례소개	• 해적, 해상 마약 밀수에 대한 임검, 수색, 나포 • 해양범죄에 대한 수색과 증거 수집 방법
27	• 연구명: The European Union as a Maritime Security Provider – the Naval Diplomacy Perspective • 연구자(연도): Larsson & Widen(2022) • 연구 목적: EU가 글로벌 안보를 위해 그 역할을 강화하고 유럽 회원국들의 군사력을 어떻게 활용해야 하는지를 평가	• 문헌연구 • 유럽회원국 웹페이지 공식 문헌 및 기록물 내용 분석 • 사례 분석 • 전문가 자문	• EU 정체성과 안보 관련 보유 자산을 분석 • EU NAVFOR 소말리아 작전과 EU NAVFOR 지중해 작전을 분석하여 해군외교의 역할이 전력 투사 이상의 효과가 있음을 확인 • 특히, 관련 작전과 임무 분석을 위해 고위 장교들을 대상으로 자문을 실행하고 내부보고서를 분석 • EU 국제해양안보의 역할 증대를 위해 국제기구, NGO, 제3국과 협력을 해야 하나 EU의 해양작전은 정치적인 면이 강하며, 이에 공통안보방위정책(CSDP)의 불확실성은 증가할 것으로 제시
28	• 연구명: A Hybrid Rule-Based and Data-Driven Approach to Illegal Transshipment Identification with Interpretable Behavior Features • 연구자(연도): Deng et al.(2022) • 연구 목적: AIS 데이터 기반의 불법 환적 식별 방법론 개발 및 활용성 검증	• 문헌연구 • 해상교통량 분석 • 불법 환적 선박 통한 특성 등에 대한 분석 알고리즘 및 계산모듈 개발 및 활용	• 불법 환적 식별 방법론 개발 • 불법 환적 선박 및 선박 통항 특성을 도출하기 위해 동적데이터전처리, 공간특성계산 모듈, 선박 접속 인식 계산 모듈, 행위특성계산 모듈, 해상교통량특성계산 모듈 등을 개발 • 프랑스 및 중국 사례지역 적용 및 활용성 검증
29	• 연구명: Maritime Transport Security • 연구자(연도): Bichou, Szyliowicz, & Zamparini(2013) • 연구 목적: 해양안보 관련 최근	• 문헌연구 • 통계분석 • 설문조사 • 전문가 자문 • 관련 정책 분	• 해양안보 도전사항, 해양안보 위협과 비용, 해양테러 발생 현황, 해적 공격 현황 등을 분석 • 미국, 캐나다, 유럽, 나이지리아, 오만, 인도, 말라카 해협, 홍콩, 모리셔스 등의 해양보안정책 현황을 소개

구분	선행연구 현황		
	연구 목적	연구 방법	주요 연구 내용
	도전사항을 분석하고 각국의 정책 현황을 소개	석 • 비교 정책 분석	하고 관련 특징을 비교 분석하여 각국의 시사점을 도출
30	• 연구명: Chapter 14. Legal Authorities for Maritime Law Enforcement, Safety and Environmental Protection • 연구자(연도): Castaneda, Condit, & Wilson(2016) • 연구 목적: 마약 밀수 및 밀매, 밀입국 등과 관련된 조직 체계 등을 분석 및 설명	• 문헌연구 • 관련 정책 및 법 분석	• 외부로부터 유입되는 마약, 불법 이민 등과 관련하여 미국 국토안보부(DHS), 국방부(DOD), 해안경비대(USCG), 세관 등 연방정부기관의 협력사항 설명 • 미 연방정부 각 기관의 기능을 설명하고 협력사항을 제시

2. 해양 복합위협 위험성 평가 설문지

제1편 응답자 기본 정보

1. 귀하의 성별은 무엇입니까?

① 남성 ② 여성

2. 귀하의 소속은 어떻게 되십니까?

① 학계 ② 연구기관 ③ 산업계 ④ 정부 및 공공기관 ⑤ 기타( )

3. 귀하의 연령대는 어떻게 되십니까?

① 20대 ② 30대 ③ 40대 ④ 50대 ⑤ 60대 이상

4. 귀하의 업무 분야에서의 총 경력 기간은 어떻게 되십니까?

① 1년 미만 ② 1년 이상~5년 미만 ③ 5년 이상~10년 미만 ④ 10년이상~15년 미만 ⑤ 15년 이상

5. 귀하의 전문 분야는 무엇입니까?

① 정책기획 ② 법집행(단속 등) ③ 테러 대응 ④ 사이버보안 ⑤ 기타( )

※ 본 연구는 해양 복합위협의 위험성 분석을 위해 USCG에서 적용하고 있는 Maritime Security Risk Analysis Model(MSRAM)을 수정·활용하여 아래의 항목에 대해 평가하고자 합니다.

- MSRAM은 Risk 분석을 위해 각 요인별로 정량 데이터를 광범위하게 활용하는 반면, 본 연구는 정량 데이터의 한계로 인해 각 요인별 위험성 분석을 위해 보유하고 있는 정량 데이터(연도별 발생 건수 및 발생 위치)와 설문조사를 통한 정성 데이터를 중심으로 위험성을 분석



제2편 해양 복합위협 개요

제2편에서는 현재 국내에서 관리하고 있는 해양위협 현황 정보와 본 연구에서 평가하고자 하는 해양 복합위협의 유형에 대한 정보를 제공합니다. 아래의 표를 확인하시고, 제3편부터 설문에 답하여 주시기 바랍니다.

❑ 해양 복합위협 유형

본 연구에서 평가하고자 하는 해양 복합위협의 유형은 다음의 표와 같으며, 이는 USCG MSRAM에서 분류하고 있는 위협의 형태를 국제범죄에 맞추어 재분류한 것입니다.

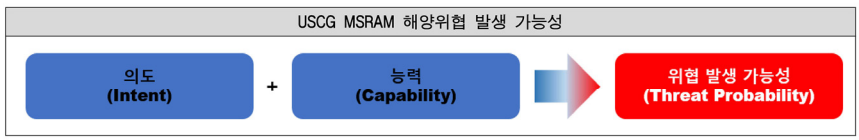
해양 복합위협 분류	USCG 공격 형태 분류	해양 국제범죄 분류	
밀입(출)국	Transfer of Terrorist	출입국문란	밀입국
			무사증
			무단이탈
			밀항
			밀출국
밀수(출)입	Transfer of weapons/materials	밀수입・출	밀수입
			밀수출
		국익・산업보호	해양산업기술보호
			지적재산침해
			불법위폐,외국환거래
		국민사회안전	원산지 허위표시
			불량식품범죄
			안전불감 범죄
			마약류 범죄
납치	Hostage Taking	인권보호	인권침해
	Hijacking of Vessel		외국인권익침해
해적 및 무장강도	Attack by Hijacked Vessel	인권보호	인권침해
	Attack by Hijacked Large Aircraft		
해양테러(연안 주요시설(발전소, 주요 항만 등) 공격, 다중이용시설(여객선, 여객터미널 등) 공격 등)	Boat Bomb	해양테러* *관련 통계는 대외비로 별도 관리	해양테러
	Boat Bomb(While vessel is present)		
	Passenger/passerby Explosives/Improvised Explosive Devices		
	Sabotage		
	Car/Truck Bomb		
드론 공격	Standoff Weapon Launched from Water and Land(including Man-Portable Air Defense Weapon)	국민사회안전	안전불감 범죄
	Small Suicide Aircraft Attack		
해저시설 공격	Swimmer/Diver/Underwater Delivery Systems	국민사회안전	안전불감 범죄
	Mines(Aquatic)		
대량살상무기	Chemical, Biological, Radiological, Nuclear	환경보존	외국선박 환경오염
사이버 공격	Cyber Attack	해양사이버범죄* *해양사이버범죄는 해양 범죄 통계에 포함하여 산정되고 있어 국제범죄가 아닌 일반 수사범죄로 분류	해양사이버범죄
기타	Ability to add additional DOD Attack modes as necessary	출입국문란	불법체류・취업
		기타	기타범죄

❑ 최근 5년(2020년-2024년) 국내 해양 위협(국제범죄) 발생 건수

분야	범죄종류	발생 건수(건)	분야별 비중
총계		1,248	100%
출입국문란	밀입국	8	28.4% (355건)
	무사증	28	
	무단이탈	4	
	밀항	12	
	밀출국	2	
	불법체류·취업	301	
밀수입·출	밀수입	77	6.3% (78건)
	밀수출	1	
국익·산업보호	해양산업기술보호	9	2.0% (25건)
	지적재산 침해	11	
	불법위폐·외국환거래	5	
국민사회안선	원산지 허위표시	121	36.1% (450건)
	불량식품범죄	86	
	안전불감 범죄	109	
	마약류 범죄	134	
인권보호	인권침해	10	4.6% (58건)
	외국인권익침해	48	
환경보존	외국선박 환경오염	162	13.0% (162건)
기타	기타 범죄	120	9.6% (120건)

제3편 해양 복합위협 발생 가능성 평가

본 편에서는 USCG MSRAM에서 활용하고 있는 해양위협의 발생 가능성 평가 모델을 활용하여 우리나라 관할 해역에서 발생할 수 있는 해양 복합위협의 발생 가능성을 평가하고자 합니다. USCG MSRAM은 해양위협의 발생 가능성을 의도와 능력으로 평가합니다.



이에 본 연구에서도 이러한 의도와 능력을 평가하기 위해 아래와 같이 해양 복합위협의 <u>의도와 능력</u>을 평가하고자 합니다.

❑ 해양 복합위협 의도

먼저 본 연구에서는 <u>우리나라 관할 해역에서</u> 해양 복합위협의 의도를 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 예시는 아래와 같습니다.

구분	척도	평가 기준	비고
1	의도 없음	실수 또는 비의도적 접근 및 접촉	위협의 목적 및 취하고자 하는 이익에 대한 달성 가능성 등을 중심으로 평가
2	매우 낮음	관심 및 정보 수집 단계 등	
3	낮음	경고 수준의 탐색 또는 시험적 접근, 실제 공격 예비단계 등	
4	보통	위협 세력이 의도를 가지고 구체적 접근 및 준비, 실제 행동 직전 단계 등	
5	높음	직접적 공격, 침입 시도, 해양시설·선박을 대상으로 한 실제 방해 행위 시작 등	
6	매우 높음	조직적으로 계획된 반복적 공격, 복합적·광범위 위협 실행 및 피해 발생 등	

위의 표와 개인의 경력을 참조하시어 <u>우리나라 관할 해역</u>에서 발생할 수 있는 <u>해양 복합위협의 의도</u>를 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 의도					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(에,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

❑ 해양복합 위협 능력

본 연구에서는 해양 복합위협의 능력을 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 예시는 아래와 같습니다.

구분	척도	평가 기준	비고
1	능력 없음	위협 실행에 필요한 인력, 장비, 경험, 기술 모두 부재. 실제 실행 불가.	위협을 실행하고자 할 때, 필요한 자원의 수급 가능성, 인력 및 기술 등 가용 수단의 접근성 등을 중심으로 평가
2	매우 낮음	기본적 자원 또는 인력 일부 보유. 위협 실행은 여러 제약(외부 지원, 제한된 범위 등)하에서만 가능.	
3	낮음	한정된 위협 유형 또는 특정 지역에서 제한적으로 실행 가능. 범위나 강도는 매우 제한적.	
4	보통	주요 해양 위협(해적, 불법조업, 테러 등)의 실행이 가능하며, 구체적 실행계획 및 일부 경험 보유	
5	높음	다양한 해양 위협을 조직적·효율적으로 실행 가능. 선문인력, 첨단기술, 실행 경험 및 성공 사례 보유.	
6	매우 높음	대규모·복합적 해양 위협을 조직적·체계적으로 반복 실행 가능. 장기적 운영 능력, 국제적으로도 위협이 될 만한 수준.	

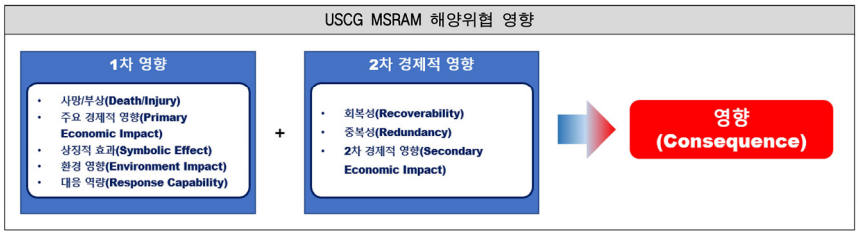
위의 표와 개인의 경력을 참조하시어 <u>우리나라 관할 해역</u>에서 발생할 수 있는 <u>해양복합 위협의 능력</u>을 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 능력					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(예,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

제4편 해양 복합위협 영향 평가

제4편에서는 우리나라 관할해역에서 발생할 수 있는 해양 복합위협의 영향을 평가하고자 합니다. USCG MSRAM은 해양위협의 영향을 평가하기 위해 인명피해, 재산피해, 상징적 효과, 국가안보 위협, 환경피해(오염 등), 정부 대응 역량 등을 1차적으로 평가합니다. 이후 피해 회복 능력, 위협의 중복성, 2차 경제피해 등을 고려하여 최종적인 해양위협 영향을 도출합니다.



다만, 본 연구에서는 이러한 다양한 영향을 평가하기 위한 위협별 인명 및 재산 피해에 관한 통계를 확보하기 어려워 인명 피해, 재산 피해, 국가 안보에 관한 영향, 환경 피해, 사회적 영향에 대한 전문가분들의 평가를 실시하고자 합니다.

❑ 해양 복합위협 인명 피해 정도

본 연구에서는 해양 복합위협의 인명 피해 정도를 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 예시는 아래와 같습니다.

구분	척도	평가 기준	비고
1	없음	인명 피해 가능성 없음	발생 가능한 인명 피해 수준을 중심으로 평가
2	매우 경미	부상자 1인 이하 발생 가능성 등 (생명에 지장 없는 경미한 상처 등)	
3	경미	경상자 2~5명 이하 발생 가능성 등 (비교적 가벼운 상처, 치료 후 회복 시간 짧음 등)	
4	보통	중상자 1명 (중대한 신체 사고 등) 또는 경상자 6~20명 발생 가능성 등	
5	심각	사망자 1명 발생 또는 중상자 2~5명 또는 경상자 20~50명 발생 가능성 등	
6	매우 심각	사망자 2명 이상 또는 중상자 5명 이상 또는 경상장 50명 이상 발생 가능성 등 (대형 참사 등)	

위의 표와 개인의 경력을 참조하시어 우리나라 관할 해역에서 발생할 수 있는 해양복합 위협의 인명 피해 정도에 대해 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 인명 피해 정도					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(예,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

❑ 해양 복합위협 재산 피해 정도

본 연구에서는 해양 복합위협의 재산 피해 정도를 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 예시는 아래와 같습니다.

구분	척도	참조 기준	비고
1	없음	인명 피해 전혀 발생하지 않음	왼쪽의 참조 피해 규모를 고려하시어 각각의 해양 복합위협이 발생했을 시 나타날 수 있는 피해규모를 평가해 주시기 바랍니다. *우리나라 「재해위로금 지급규정」은 기타 재산피해에서 소규모 피해를 50만원초과 1,000만원 이하, 대규모 피해를 1,000만원 초과인 경우로 구분
2	매우 경미	1천만원 미만의 피해	
3	경미	1천만원 이상 1억원 미만 피해	
4	보통	1억원 이상 10억원 미만 피해	
5	심각	10억언 이상 50억원 미만	
6	매우 심각	50억원 이상의 피해	

위의 표와 개인의 경력을 참조하시어 우리나라 관할 해역에서 발생할 수 있는 해양복합 위협의 재산 피해 정도에 대해 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 재산 피해 정도					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(예,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

❑ 해양 복합위협 국가 안보 영향

본 연구에서는 해양 복합위협의 국가 안보 영향을 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 기준은 아래와 같습니다.

구분	척도	평가 기준
1	없음	국가 안보에 전혀 영향을 미치지 않음. 지역적/일상적 수준에만 머물러 국가 기능에는 영향 없음.
2	매우 경미	일부 지역, 특정 집단 또는 소규모 자원 등에 제한적으로 영향. 국내 일부 보안 강화 필요.
3	경미	중요한 해양 인프라, 해상교통, 특정 산업 등에 부분적 위협 발생. 일시적 정책 변화 또는 경계조치 필요.
4	보통	경제활동, 전략적 자원, 국경・주변 해역 등 국가 핵심 이익 일부에 실질적 위협. 정책조정, 다부처 협력 및 군사적 대비 필요.
5	심각	국가 안보정책, 에너지・무역 등 광범위한 분야에 직접 타격. 국가 자산, 군사력, 대외정책 전반의 총력 대응 필요. 국내 비상대응 체계 가동.
6	매우 심각	국가의 존립 기반(주권・영토・국민 생존 등)에 중대한 위협 유발. 국가적 비상사태, 국제협력 요청 및 장기적 위기 대응 필요.

앞의 표와 개인의 경력을 참조하시어 우리나라 관할 해역에서 발생할 수 있는 해양복합 위협의 국가 안보 영향에 대해 대해 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 국가 안보 영향					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(예,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

❑ 해양 복합위협 환경 피해

본 연구에서는 해양 복합위협의 환경 피해 영향을 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 기준은 아래와 같습니다.

구분	척도	평가 기준
1	없음	환경적 피해가 발생하지 않음. 해양 생태계 및 자원 변화 없음.
2	매우 경미	국지적・일시적 피해 발생(일부 해양생물, 소규모 해역만 영향). 자연적 복구 가능.
3	경미	제한된 해양 생태계, 자원, 어업활동 등에 피해. 복구・회복에 단기적 인적・자원 투입 필요.
4	보통	주요 해역, 해양생물군, 수산자원 등에 현저한 피해 발생. 복구・회복에 장기간 및 조직적 대응 필요.
5	심각	대규모 해역 오염, 어장 파괴, 서식지 및 보호종 집단 피해. 경제・생태계 전반에 장기적 악영향 초래.
6	매우 심각	국가・국제적 해양생태계에 회복 불가능한 손상. 장기간 경제・지리적, 생태적 위기 상황 유발. 국제 기준 위반, 대규모 대응 필요.

앞의 표와 개인의 경력을 참조하시어 우리나라 관할 해역에서 발생할 수 있는 해양복합 위협의 환경 피해에 대해 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 환경 피해					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(예,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

❑ 해양 복합위협 사회적 영향

본 연구에서는 해양 복합위협의 사회적 영향을 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 기준은 아래와 같습니다.

구분	척도	평가 기준
1	없음	사회적 피해, 불안 또는 변화 없음. 일상생활과 지역사회 정상 유지.
2	매우 경미	일부 지역・개인에 국한된 단기 불안, 여론의 일시적 관심. 사회 구조와 기능 변화 없음.
3	경미	국지적 집단・업계에 직접적 불안, 소규모 경제적 손실, 지역사회 내 갈등・불신 초래.
4	보통	지방・산업계, 어업・관광 등 특성 분야에서 지속적 불안감, 신뢰 하락, 사회적 긴장 확대.
5	심각	국가적 여론 악화, 정책 변화 요구, 광범위한 경제・사회적 혼란 유발.
6	매우 심각	국가 전체에 사회적 대립・패닉, 비상사태 선포 필요, 장기적 가치관 및 생활방식 변화, 사회적 복구에 장기간 소요.

앞의 표와 개인의 경력을 참조하시어 <u>우리나라 관할 해역</u>에서 발생할 수 있는 <u>해양복합 위협의 사회적 영향에</u> 대해 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 사회적 영향					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(예,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

제5편 해양 복합위협 취약성 평가

제5편에서는 우리나라 관할해역에서 발생할 수 있는 해양 복합위협에 대한 취약성을 평가하고자 합니다. USCG MSRAM은 해양위협에 대한 취약성을 평가하기 위해 위협의 실행 가능성, 선주 및 운항자의 시스템 보안, 법집행기관의 시스템 보안, USCG의 시스템 보안, 공격 대상의 을 별도로 평가하여 취약성을 도출합니다.



이를 참고하여 본 연구에서는 우리나라 관할해역에서 발생가능한 해양 복합위협의 실행 가능성과 우리나라 정부의 보안 체계 수준, 위협 대상의 방어 능력을 평가하고자 합니다.

❑ 해양 복합위협 실행 가능성

본 연구에서는 해양 복합위협의 실행 가능성을 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 기준은 아래와 같습니다.

구분	척도	평가 기준
1	실행 가능성 없음	자원, 의도, 조건, 동기 모두 결여. 위협 실행 가능성 없음.
2	가능성 매우 낮음	제한적 자원 또는 조건 일부 존재. 사실상 실현 가능성 극히 낮음.
3	낮음	위협 실행에 필요한 최소 요건(자원・기술 등) 일부 충족. 특정 상황에 한해 소규모 시도 가능성이 존재.
4	가능성 보통	주요 조건・자원・동기 등 상당 부분 충족. 환경이 맞을 경우 현실화 가능성 존재.
5	높음	대부분의 필요 조건 충족, 구체적 계획・준비 갖추어 실행 직전 단계. 매우 높은 실행 현실성.
6	실행	모든 조건을 충족하여 실제로 해양위협이 실행 가능한 상태

앞의 표와 개인의 경력을 참조하시어 우리나라 관할 해역에서 발생할 수 있는 해양복합 위협의 실해 가능성에 대해 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 달성가능성					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(예,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

❑ 해양 복합위협 정부 보안 체계 역량

본 연구에서는 해양 복합위협의 정부 보안 체계 역량을 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 기준은 아래와 같습니다.

구분	척도*	평가 기준
1	대응 역량 매우 높음	선진국 수준의 예·경보, 선제적 예방 활동, 지속적 정책·기술 혁신. 국제 협력, 모범 보안 사례 창출·확산, 모든 해양위협에 대한 완벽한 대응·회복·지속 개선 체계 구축.
2	높음	국제 기준(ISPS Code 등)과 전문 인력, 첨단 기술 활용. 신속한 사고 탐지·대응·복구 및 광범위한 해양 위협에 대한 통합적 통제 능력 보유. 타 부처 및 민간과 협력 체계 갖춤.
3	보통	주요 해양 분야별(선박·항만·디지털 시스템 등) 맞춤형 보안 정책, 사고 대응 체계 구축. 정기적 진단·훈련 실시, 실질적 사고 발생 시 통제·회복 가능.
4	낮음	일부 분야(선박, 항만 등)에 제한적 보안 체계·지침·기술 도입. 기본 대응·모니터링 가능하나 상시 점검·업데이트 부족.
5	매우 낮음	기본적인 정책 또는 최소한의 대응 조직 존재. 역할·기능 매우 제한적, 위협 발생 시 효과적 대응 불가.
6	대응 역량 없음	보안 체계와 정책, 대응 조직 모두 부재. 해양위협 인식과 대응 불가

*** 주의. 대응 역량이 높을 수록 낮은 척도, 대응 역량이 낮을 수록 높은 척도를 부여**

앞의 표와 개인의 경력을 참조하시어 **우리나라 관할 해역**에서 발생할 수 있는 **해양복합 위협에 대한 정부 보안 체계 역량을** 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 정부 대응 역량					
	1	2	3	4	5	6
밀입(출)국						
밀수(출)입						
납치						
해적 및 무장강도						
해양테러						
드론 공격						
해저시설 공격						
대량살상무기						
사이버 공격						
기타 해양 복합위협(예.)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

❑ 해양 복합위협 대상의 방어능력

본 연구에서는 해양 복합위협 대상의 방어능력을 아래와 같은 척도로 평가하고자 합니다. 각 척도에 따른 구체적인 평가 기준은 아래와 같습니다.

구분	척도*	평가 기준
1	매우 강함	국가・군사적 수준의 방어 체계, 실시간 대응・차단. 대규모・첨단 공격에도 사실상 침투 불가능, 최상위 보호 수준.
2	강함	다층적・복합적 방어시스템(물리・전자・인적 방어 결합)과 신속 대응 체계. 조직적 공격에도 높은 저항력.
3	보통	강화된 보안(복합감시, 출입통제시스템, 경고장치 등) 적용. 숙련된 공격자만 침투 가능.
4	취약	표준적 보안 체계(경비, CCTV, 일부 출입통제 등) 도입. 공격자는 일정한 노력만으로 침투 가능.
5	매우 취약	기초적 방어만 존재(문, 잠금장치, 경비원 등). 공격/침투에 거의 저항력 없음
6	방어 역량 없음	보호장치, 감시, 경비 등 방어 수단 전혀 없음. 누구나 쉽게 침투・공격 가능.

* 주의. 방어 능력이 높을수록 낮은 척도, 방어 역량이 낮을수록 높은 척도를 부여

앞의 표와 개인의 경력을 참조하시어 **우리나라 관할 해역**에서 발생할 수 있는 **해양 복합위협 대상의 방어능력을** 평가해주시기 바랍니다.(해양복합 위협별 해당하는 척도에 동그라미(O) 또는 체크(✓)를 표시.)

해양 복합위협 분류	해양 복합위협 정부 대응 역량					
	1	2	3	4	5	6
밀입(출)국 (주요 위협 대상 : 해안선, 연안, 항만, 선착장, 선박, 해양시설 등)						
밀수(출)입 (주요 위협 대상 : 해안선, 연안, 항만, 선착상, 선박, 해양시설 등)						
납치 (주요 위협 대상 : 선박 및 선원, 해양시설 및 그 종사자 등)						
해적 및 무장강도 (주요 위협 대상 : 선박 및 선원, 해양시설 및 그 종사자 등)						
해양테러 (주요 위협 대상 : 국가 주요 해상 인프라(발전소 등), 무역항 및 항만시설, 유조선 등 전략 자원 운송 선박, 다중이용시설(여객선 터미널 등))						
드론 공격 (주요 위협 대상 : 항만, 터미널, 선박 등)						
해저시설 공격 (주요 위협 대상 : 해저케이블 등)						
대량살상무기 (주요 위협 대상 : 국가 주요 해상 인프라(발전소 등), 연안지역 주요 국가 시설(터미널, 해양경찰서 등) 등)						
사이버 공격 (주요 위협 대상 : 선박 운항 시스템, 해운선사 관제시스템, 해상교통 국가시설(해상교통관제센터 등), 항만물류 시스템 등)						
기타 해양 복합위협(예,)*						

* 필요시 발생가능한 기타 해양 복합위협을 표시해 주시고 그 척도를 평가해 주세요.(없다면 평가를 제외해주세요)

제6편 기타 의견

본 편에서는 본연구와 관련하여 귀하의 의견을 자유롭게 제시해 주시면 감사하겠습니다.

표 안에 의견을 작성해 주세요.

…

본 설문에 끝까지 응답해 주셔서 대단히 감사합니다.

기본연구보고서 발간목록

2025년

01	청색경제 이행지표 개발 및 투자효과 분석	김주현
02	해양문화산업의 지역 경쟁력 진단과 발전전략 연구	이슬기
03	유해·교란 해양생물 지정 제도 개선방안 연구	정여진
04	해양보호구역의 효과적 관리 방안 연구	김미주
05	해양 복합위협의 실효적 대응 방안 연구	민영훈
06	해양 위성정보 활용 방안 연구	조성진
07	수산업 정책 전주기 연계성 강화 방안 연구	안지은
08	소비자 맞춤형 식품시장 성장에 따른 수산식품산업 대응 방안 연구	임경희
09	외국인 어선원 확보를 위한 제도 개선 연구	정명화
10	수산식품 물가 안정화 방안 연구	박혜진
11	수산물 업사이클링 생태계 조성 방안 연구	이남수
12	어촌과 연안의 통합적 발전을 위한 바다생활권 도입방안 연구	박상우
13	해운 얼라이언스 재편에 따른 영향분석과 대응방안 연구	김병주
14	연안대중교통의 운영 효율성 제고를 위한 정책 연구	류희영
15	그린 암모니아 선박 연료 전환 대응 방안 연구	전서연
16	스마트항만 기술 수용성 제고를 위한 법·제도 개선 방안 연구	이다예
17	탄소중립항만 전환을 위한 항만하역장비 관리체계 개선 방안 연구	이혜령
18	부산항 중장기 발전전략 연구	김근섭
19	재난 · 재해 대비 항만 위험물 컨테이너 물류공급망 대응 방안 연구	최나영환
20	국제물류시장 공정경쟁질서 확립 방안 연구	김동환

2024년

01	섬·바다·강 연계 관광 네트워크 구축방안 연구	최일선
02	해양 스타트업 실패 자산화 방안 연구	좌미라
03	시민친화적 바닷가 공간 조성에 관한 연구	정지호
04	연안이용 관리 법제 정비방안 연구	최석문
05	특별관리해역 관리제도 재편 방안 연구	최수빈
06	해양관할구역 과세권한의 체계적 배분방안 연구	이혜영
07	어업인의 디지털 전환 수용성 제고방안 연구	오서연
08	수산물 무역(수출입) 단기 전망모형 구축 연구	한기욱
09	어촌소멸에 따른 사회경제적 영향분석과 대응전략 연구	이상규
10	어촌다움에 기반한 어촌공간관리 방안 연구	이승혜
11	파생상품을 이용한 해운선사의 위험관리에 관한 연구 - 운임선도거래(FFA)를 중심으로 -	김한나
12	내항상선 해양사고 경감방안 연구	허성례
13	항만재개발사업 공공성 강화 방안 연구	김세원
14	해외 항만터미널 확보 전략 연구	김근섭
15	항만 하역능력의 서비스 수준 개선 연구	이화섭
16	국내 무역항 거버넌스 체계 개편방안 연구	김근섭
17	선박의 원격운항을 위한 제도 개선방안 연구	박혜리
18	국제물류기업 육성을 위한 법제 개선방안 연구	최나영환
19	글로벌 공급망 리스크 대응 정책효과 분석 모형 개발 연구	강무홍
20	한-북미 무역구조 분석 및 물류공급망 변화 대응방안 연구	이성우

수시연구보고서 발간목록

2025년

01	해양치유시설 조성·운영 제도 개선 연구	이정아
02	국제 해양질서 전환 대응 해양대외전략 기반 연구	박수진
03	유기수산식품 국제 동등성 확보 방안	오서연
04	선원 복지 개선방안 연구 - 선내 급식을 중심으로	허성례
05	항만재개발사업 추진 체계 재정립 연구 - 항만재개발사업 업무 매뉴얼 개선을 중심으로	김세원
06	군소도서국 해양수산 국제협력 방안 수립	전혜은
07	어촌발전특구 도입을 위한 법·제도 연구	박상우
08	해양생태계서비스 활용 방안 연구	정세미
09	해양에너지 산업 활성화 방안 연구	육근형
10	비관리청항만개발사업 정보화 정책 방향 연구	이종필
11	해양안보 위협지수 개발 및 활용방안 연구 - 선박 이상 행위를 중심으로	민영훈
12	지방관리무역항 보안관리체계 재정립 연구	김가현
13	부산항 터미널 위험물 컨테이너 장치 효율 개선 방안 연구 - 법·제도 측면 -	김우선
14	새만금호 수질관리 강화 방안 연구	장원근
15	미 상호주의 대응 수산분야 비관세장벽 영향 연구	이정미
16	수중레저 안전관리 체계 정비를 위한 제도개선 연구	이정아

2024년

01	해양정보산업 진흥을 위한 제도 개선 방안 연구	김찬웅
02	한-아프리카 국제수산협력 체계 개선 연구	이채령
03	해양안보 MDA 체계 구축·활용 방안 연구	민영훈
04	인천항 자유무역지역의 효과적 운영을 위한 전략 방안	한장협
05	해양문화자원을 활용한 연안도시활력 증진 방안 연구	이슬기
06	부산항 물동량 유치방안 연구	김은우
07	국제사회의 대북제재 동향과 우리의 대응:해양수산분야를 중심으로	채수란
08	국내 연안여객선 관광·이용 활성화 방안 연구	이정아
09	내수면어업 허가·신고 제도 개선방안 연구	최순
10	어업선진화를 위한 어업관리체계 개편방안	심성현
11	글로벌 공급망 변동에 따른 해운물류 지원방안	황수진
12	연안 중소선사의 탄소중립 달성을 위한 친환경정책 지원방안	류희영
13	항만기술산업 활성화를 위한 법제도 정비 방안 연구	김보경
14	해양모태펀드 투자활성화 방안 연구	한기원
15	특별관리해역 내 공공하수처리시설의 방류수 수질기준 강화방안	장원근
16	중대재해처벌법 대응 양식장 안전성 개선 방안 연구	윤미경
17	국가관리연안항 발전전략 수립체계 연구	신정훈
18	글로벌 공급망 대응 해운항만물류 전문인력 양성 발전방안 연구	권보배
19	해양수산 국제개발협력 중장기 전략 연구	전혜은

일반연구보고서 발간목록

2025년

01	해양수산 공공데이터 플랫폼 활용 제고 방안 연구	김성은
02	동아시아 해양플라스틱 오염 대응 재원 조성 방안	이윤정
03	한-아세안 해양협력 전략적 강화방안 연구	최지연
04	수산업 강제노동 규범화 대응체계 구축연구	박찬엽
05	해조류 활용 신산업 생태계 조성 방안 연구	조헌주
06	미국 무역환경 변화와 해운·조선산업의 영향 분석 연구	김한나
07	해상운임에 대한 지정학적 리스크의 전이효과 분석	최영재
08	스마트항만 개발 효과 산정 방법론 연구	안승현
09	항만 수급분석 체계화 및 지침 마련 연구	신정훈
10	비컨테이너 부두 하역능력 산정을 위한 적정 점유율 기준 연구	이화섭
11	국가 스마트 콜드체인 물류거점센터 구축연구	조지성
12	해운항만물류 전문인력 중개 플랫폼 모델 개발	권보배
13	미국 이력 추적 의무화에 따른 수산물 수출기업 대응실태 분석 연구	박혜진
14	AI 활용 글로벌 수산이슈 및 무역전망체계 고도화 연구	한기욱
15	섬어촌 디지털 정보격차 해소를 위한 정책연구	이상규

2024년

01	한-북극권 청색경제 협력사업 추진 방안	김엄지
02	전환기 글로벌 해양환경규범의 대응력 강화 연구	박수진
03	해양 지속가능성 시범 평가 연구	최희정
04	Scope 3 기준 원양산업 탄소배출추정 및 대응방안 연구 - 원양저연승어업을중심으로	조헌주
05	수산물 공급망 관리 개선방안 연구(한태 무역을 중심으로)	한기욱
06	신통상규범 확대에 따른 수산분야 영향 및 대응방안	박혜진
07	탄소배출 규제 대응을 위한 컨테이너 선대 교체 수요 추정 연구	최건우
08	연안항개발사업의 경제적 편익에 관한 연구	김성아
09	한국과 미동부 항만 간 녹색해운항로 구축방안 연구	김가현
10	비컨테이너 항만물동량 예측모형 고도화 방안 연구(Ⅲ) - 철광석,화학공업생산품,기타광석,잡화를중심으로	이나영
11	접안 대기시간 감소에 따른 탄소집약도지수(CII) 변화 분석	김보람

기본연구 2025-05

해양 복합위협의 실효적 대응 방안 연구

인 쇄 2025년 12월 29일
발 행 2025년 12월 31일

발 행 인 조 정 희
발 행 처 한국해양수산개발원
주 소 49111 부산시 영도구 해양로 301번길 26(동삼동)
연 락 처 051-797-4800 (FAX 051-797-4810)
등 록 1984년 8월 6일 제313-1984-1호

조판·인쇄 ㈜대주애드 (051-803-6630~1)

판매 및 보급: 정부간행물판매센터 Tel: 02-394-0337
정가 15,000원

해양 복합위협의 실효적 대응 방안 연구

A Study on Effective Countermeasures against Maritime Hybrid Threats

KMI 한국해양수산개발원
KOREA MARITIME INSTITUTE

49111 부산광역시 영도구 해양로301번길 26 (동삼동)
TEL. 051-797-4800 FAX. 051-797-4810

값 15000 원
93300
9 791168 662957
ISBN 979-11-6866-295-7