Maritime Cyber Threat White Paper 2026

February 19, 2026

CYTUR Inc.

[Prologue]

CYTUR
Cyber Trust & Resilience for Maritime

싸이터는 설계 단계부터 보안을 내재화하는 'Secure by Design' 철학을 기반으로, 선박의 발주·계약, 설계, 건조, 시운전, 그리고 사후에 이르는 전 과정을 보호하는 통합 사이버보안 관리 솔루션과 서비스를 제공하는 해양·선박 사이버 보안 전문 기업입니다.

CYTUR(Cyber Trust & Resilience)에 담긴 의미처럼, 우리는 디지털 전환의 파도를 맞이한 해양 산업에 사이버 신뢰와 회복 탄력성을 제공하는데 집중하고 있습니다.

2026 해양 사이버위협 백서:
데이터 기반의 해사 방어 전략

1. 백서 발간의 목적

오늘날 해양 산업은 디지털 전환의 가속화로 인해 이전과는 전혀 다른 형태의 사이버 위협에 직면해 있습니다. 하지만 폐쇄적이고 특수한 해양 환경의 특성상, 신뢰할 수 있는 위협 데이터와 분석 자료를 찾기란 매우 어려운 것이 현실입니다.

본 백서는 이러한 정보의 불균형을 해소하고, 해양 산업 관계자들이 고도화되는 사이버 위협을 정확히 파악하여 선제적으로 대비할 수 있도록 기획되었습니다.

2. 주요 내용 및 구성

이 백서는 해양 특화 위협 인텔리전스 솔루션인 CYTUR-TI 를 통해 수집된 실제 데이터를 기반으로 작성되었습니다. 2024 년부터 2025 년 현재까지의 해사 전반에 걸친 위협 정보와 최신 트렌드를 심층 분석하여 담았습니다.

3. 독자들에게 보내는 메시지

사이버 보안은 단순히 사고를 막는 기술을 넘어, 스마트 선박의 안전 운항과 비즈니스 연속성을 보장하는 핵심 경쟁력입니다. 특히 설계 단계부터 보안을 고려하는 'Secure by Design'을 실현하기 위해서는 정확한 위협 정보가 그 출발점이 되어야 합니다.

정보가 부족한 해양 사이버 보안 분야에서 본 백서가 막연한 불안감을 확신으로 바꾸고, 더욱 안전한 해양 디지털 생태계를 구축하는 데 실질적인 이정표가 되기를 바랍니다. CYTUR 는 앞으로도 해양 산업의 든든한 디지털 파수꾼으로서 가치 있는 정보를 지속적으로 공유할 것을 약속 드립니다.

스마트 해양 시대를 위한 필수:
왜 해양 전문 CTI 인가?

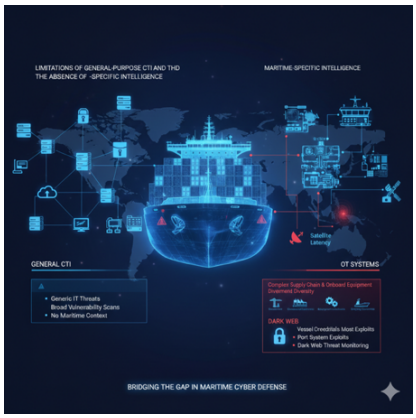
해양 디지털 전환(DX)과 확장된 공격 표면(Attack Surface)

오늘날 조선 해양 산업은 거대한 디지털 전환(DX)의 파도를 맞이하고 있습니다. 스마트 선박의 등장으로 선박성능 모니터링 및 이상 징후 사전 관리(Predictive Maintenance) 를 위한 데이터 트래픽이 폭발적으로 증가했습니다.

그러나 이러한 연결성의 확대는 양날의 검과 같습니다. 과거 고립된 환경에 있던 선상 제어 시스템(OT)이 위성 통신을 통해 육상 네트워크(IT)와 긴밀하게 연결되면서, 사이버 공격자가 침투할 수 있는 공격 표면(Attack Surface)은 전례 없이 확장되었습니다.

특히 데이터가 육상과 선박 사이를 끊임없이 오가는 과정에서 보안 취약점이 노출될 가능성이 커졌으며, 이는 단순한 데이터 유출을 넘어 선박의 안전 운항을 직접적으로 위협하는 요소가 되고 있습니다.

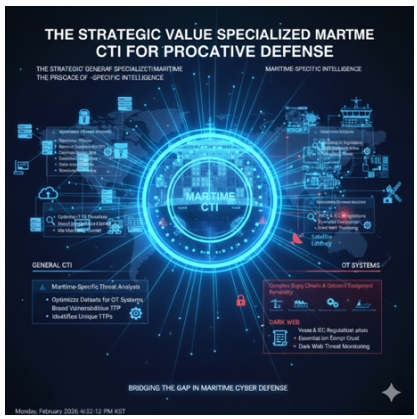
범용 CTI 의 한계와 해양 특화 정보의 부재



현재 많은 기업이 범용적인 사이버 위협 인텔리전스(CTI) 서비스를 이용하고 있으나, 해양 산업의 특수성을 고려할 때 그 한계는 명확합니다. 일반적인 IT 중심 CTI 는 선박 고유의 통신 프로토콜인 NMEA, AIS, CAN 버스 등에 대한 깊이 있는 분석을 제공하지 못합니다.

또한, 위성 통신 특유의 지연 시간(Latency)이나 대역폭 제한 등 해상 통신 환경을 이해하지 못한 분석은 실질적인 대응책이 되기 어렵습니다. 특히, 다크 웹(Dark Web) 등 비공개 웹 영역에서 거래되는 선박 접근 권한이나 항만 운영 시스템의 취약점 정보는 더욱 큰 위협이 되고 있습니다.

선제적 방어를 위한 전문 CTI 의 전략적 가치



해양 전문 CTI 는 단순히 침입을 탐지하는 것을 넘어, 위협이 실현되기 전 선제적으로 대응하는 데 목적이 있습니다.

해양 특화 위협 분석

해상 환경에 최적화된 데이터셋을 바탕으로, 선박 OT 시스템을 타깃으로 하는 고유한 위협 패턴과 전술(TTPs)을 식별합니다.

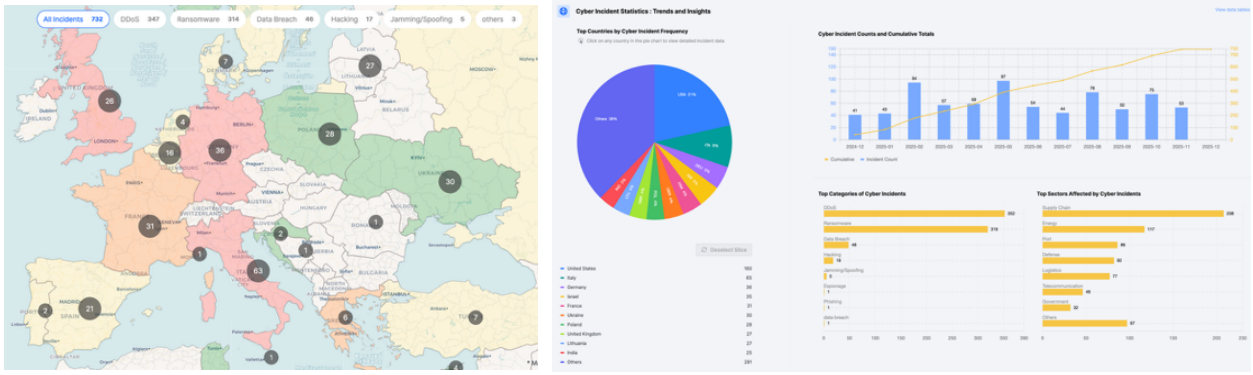
국제 표준 준수 및 신뢰도 확보

IMO(국제해사기구) 및 IEC 표준 등 갈수록 강화되는 글로벌 사이버 보안 규제에 대응하기 위해서는 신뢰할 수 있는 특화 인텔리전스가 필수적입니다.

결국, 변화하는 해양 위협 지형에서 선박과 자산을 보호하기 위한 핵심은 "해양의 언어를 이해하는 인텔리전스"를 확보하는 것입니다. 해양 특화 CTI 는 단순한 보안 도구가 아닌, 스마트 선박의 안전한 운항과 지속 가능한 비즈니스를 보장하는 전략적 자산이 될 것입니다.

CYTUR-TI(Threat Intelligence): 해양 특화 사이버 위협 인텔리전스

[핵심 기능 및 특장점]



▲ CYTUR-TI™

1. 해양 특화 위협 데이터 분석

전 세계 해상에서 발생하는 사이버 공격 사례와 해킹 그룹의 동향을 분석합니다. 특히 선박의 주요 통신 프로토콜(NMEA, AIS 등) 및 선상 제어 시스템(OT)의 취약점 정보를 집중적으로 수집하여 해양 산업에 최적화된 인텔리전스를 제공합니다.

2. 딥, 다크 웹 모니터링

검색 엔진으로 접근이 불가능한 다크 웹 포럼, 마켓, 그리고 비밀 메신저 채널을 실시간 모니터링합니다. 선박의 접속 권한 거래, 탈취된 승무원 계정 정보, 선박 설계 도면 유출 등 해양 자산과 직접적인 연관이 있는 위협 징후를 조기에 식별합니다. 자사 선박이나 선사를 향한 구체적인 공격 계획이 포착될 경우, 즉시 보안 담당자에게 경보를 발령하여 보안 정책을 즉각적으로 강화할 수 있게 합니다.

3. 내·외부 데이터 융합 기반의 지능형 통합 진단

CYTUR-TI™ 는 선박의 상태 데이터를 실시간으로 감시하는 자사 CYTUR-NS 와 CYTUR-TA 솔루션과 유기적으로 연동하여 외부의 위협 정보(TI)와 내부 장비의 상태 정보(OT)를 통합 분석함으로써, 단순한 기계적 결함인지 외부 공격에 의한 오작동인지를 명확히 판별해 줍니다.

[도입 효과 및 비즈니스 가치]

1. 사이버 복원력 강화

공격자가 선박 시스템을 공격하기 전에 침입 경로를 차단함으로써 선박의 운항 안전성과 비즈니스 연속성을 확보합니다.

2. 사후 관리 비용 절감

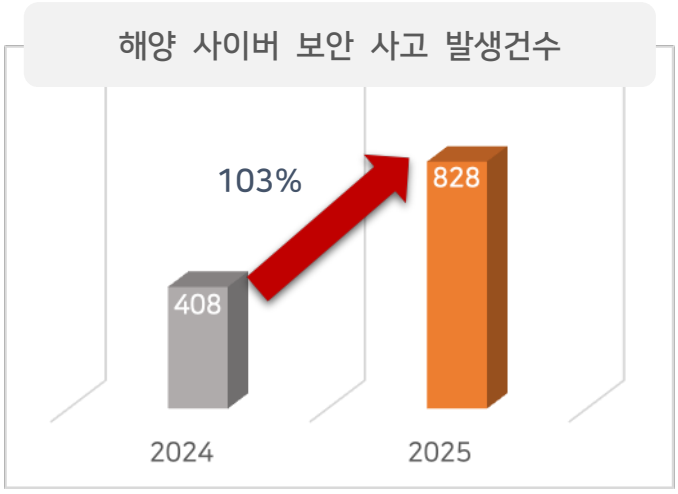
사고 발생 후 대응하는 방식에서 벗어나 위협을 미리 탐지함으로써, 대규모 데이터 유출이나 시스템 마비로 인한 막대한 복구 비용 리스크를 최소화합니다.

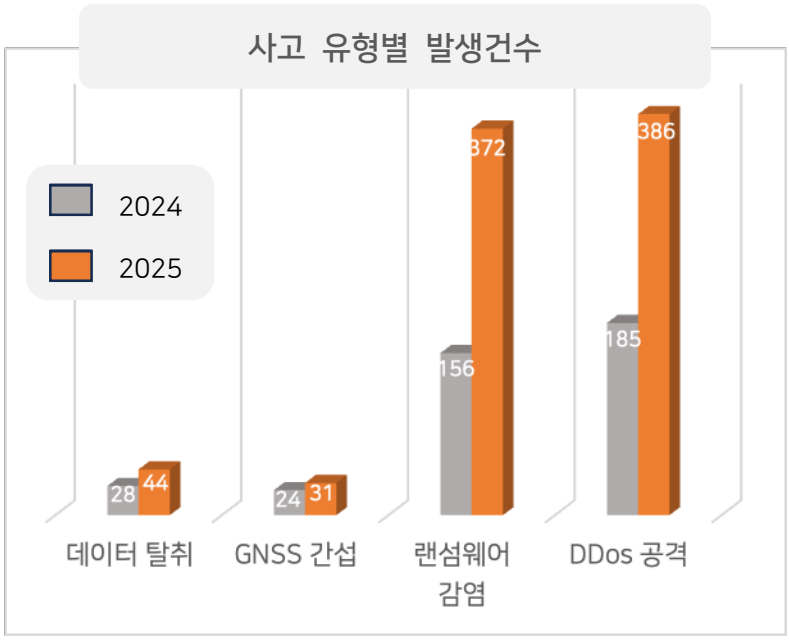
3. 글로벌 규제 대응

IMO MSC-FAL.1/Circ. 3 과 IACS UR E26/E27 등 최신 국제 해양 보안 표준에서 요구하는 위협 모니터링 및 대응 능력을 가장 효과적으로 입증할 수 있습니다.

해양 사이버위협 Overview

2024 년 대비 2025 년 해양 사이버 사고 건수는 103% 급증하며 해상 안전의 중대한 위협으로 부상했습니다. 공격 유형으로 서비스 거부(DDoS)와 랜섬웨어, 악성코드 감염이 대부분을 차지하며 증가폭 또한 2 배 이상 증가하였습니다.





해양 사이버위협 유형의 특성

1. 랜섬웨어 및 악성코드 감염(Ransomeware/Malware)

- 공격 경로:
  승무원에게 발송된 피싱 이메일의 첨부파일, 보안이 취약한 선내 공용 Wi-Fi, 검증되지 않은 USB 메모리 사용을 통해 내부망으로 확산됩니다.

- 특성:
  선박 관리 시스템(PMS) 데이터를 암호화하여 운항 기록을 인질로 잡고 금전을 요구합니다.

2. 분산 서비스 거부 공격(DDos)

- 공격 경로:
  보안 설정이 미비한 IoT 장비나 선내 통신 단말기를 봇넷(Botnet)으로 포섭한 뒤, 특정 시간에 위성 통신 대역폭에 무차별적인 트래픽을 발생시켜 마비시킵니다.

- 특성:
  육상 관제 센터와의 연결을 차단하여 고립된 선박의 위기 대응 능력을 상실시킵니다. 또한 NoName057(16)등 핵티비스트 그룹의 항만, 정부기관 대상으로 공격도 지속되고 있습니다.

3. GPS 스푸핑 및 재밍 (GPS Spoofing/Jamming)

- 공격 경로:
  외부에서 강력한 전파 방해 신호를 쏘거나(재밍), 실제 위성 신호보다 강한 허위 신호를 송출(스푸핑)하여 안테나 수신기를 기만합니다.

- 특성:
  항해 장비(ECDIS, AIS)에 가짜 위치 정보를 표시하여 선박을 의도적으로 경로에서 이탈시키거나 영해 침범을 유도합니다.

4. 데이터 탈취 및 정보 유출 (Data Breach)

- 공격 경로:
  육상 네트워크와 연결된 선박용 클라우드나 원격 유지보수 채널의 취약점을 공략하여 서버에 저장된 기밀 정보를 탈취합니다.

- 특성:
  선박 설계 도면, 운항 정보, 화물 적하 목록, 승무원 개인정보 등을 탈취하여 다크웹에 판매하거나 2 차 정밀 공격의 기반으로 활용합니다.

5. OT(운영 기술) 시스템 침투 및 제어권 탈취

- 공격 경로:
  보안 경계가 모호한 IT-OT 통합망의 접점을 뚫고 들어가 엔진 제어(IAS), 평형수 관리(BWMS) 등 핵심 제어 장치에 직접 명령을 내릴 수 있으며 선박 통신시스템(VSAT), 항해 시스템(ECDIS)에 대상 공격이 증가하고 있습니다.

- 특성:
  선박의 물리적 거동을 강제로 제어함으로써 충돌, 좌초, 환경 오염 등 재난 수준의 사고를 직접 유발할 수 있습니다.

해양 사이버위협 지역별 특성 분석

해양 사이버 위협이 지역별로 다양한 양상을 보이고 있습니다. 각 해역을 둘러싼 지정학적 이해관계와 경제적 가치가 다르기 때문입니다. 호르무즈 해협이나 발트해와 같은 분쟁 지역에서는 국가적 차원의 군사적ㅇ정치적 목적을 달성하기 위해 GPS 조작이나 전파 방해와 같은 시스템 교란 행위가 주로 발생합니다.

반면, 물동량이 집중되는 아시아 해역이나 글로벌 거점 항만에서는 경제적 이익을 극대화하려는 범죄 조직에 의해 데이터 탈취 및 랜섬웨어 공격이 빈번하게 나타납니다.

결과적으로 해상 사이버 위협은 단순한 기술적 해킹을 넘어, 각 지역의 특수성이 투영된 복합적인 형태로 전개되고 있습니다.

1. **중동 - 호르무즈 해협, 페르시아만**
   이 지역은 지정학적 긴장이 매우 높습니다. 최근에는 유조선의 GPS 신호를 조작(스푸핑)하여 배가 실제로는 공해상에 있음에도 불구하고 특정 국가의 영해 안에 있는 것처럼 시스템을 속이는 수법이 자주 발견됩니다.

   이는 선박을 강제로 멈추거나 나포하기 위한 명분을 만드는 데 사용됩니다.

2. **아시아 – 말라카 해협 및 남중국해**
   전 세계 물동량의 핵심인 이 지역에서는 '사이버 해적'이 기승을 부립니다. 과거에는 무작정 배를 습격했다면, 이제는 선사의 네트워크를 해킹해 어떤 배에 값비싼 화물이 실렸는지, 보안 요원은 몇 명인지 미리 파악한 뒤 타겟을 정해 공격합니다.

3. **유럽 – 발트해 및 흑해 연안**
   우크라이나-러시아 전쟁 등의 영향으로 광범위한 전파 방해가 일상화되어 있습니다. 민간 선박들이 이 지역을 지날 때 갑자기 GPS 가 먹통이 되거나 위치가 수백 km 떨어진 곳으로 표시되는 현상이 빈번하며, 이는 해상 사고의 직접적인 원인이 됩니다.

4. 글로벌 주요 항만 - 로테르담, LA, 부산등

대형 항만 터미널은 '랜섬웨어'의 주요 타겟입니다. 항만 운영 시스템(TOS)을 암호화하여 컨테이너 하역을 전면 중단시키고 거액의 몸값을 요구합니다. 한 곳의 항만만 마비되어도 글로벌 공급망 전체에 병목 현상이 발생하기 때문입니다.

해양 사이버위협 기자재별 특성 분석

선박 기자재 대상 사이버 위협은 해당 장비가 담당하는 기능에 따라 항해 안전, 선박 제어, 화물 관리 등 각기 다른 피해 양상으로 나타납니다. 따라서 선박의 안전운항을 확보하기 위해서는 IT 와 OT 시스템이 결합된 각 기자재의 고유한 취약점을 이해하고, 그에 따른 차별화된 보안 대응 체계를 구축하는 것이 필수적입니다.

1. 항해 및 통신 시스템 (Navigation & Communication)

가장 직접적인 물리적 사고(충돌, 좌초)를 유발할 수 있는 핵심 기자재들입니다.

(1) GNSS/GPS 수신기

- 위협 특성 : 가짜 신호를 보내 위치를 오인하게 만드는 스푸핑(Spoofing)이나 신호를 차단하는 재밍(Jamming)에 매우 취약합니다.
- 사고 영향 : 선박이 계획된 경로를 이탈하거나, 인접 국가의 영해를 무단 침범하게 되어 나포 및 외교적 분쟁의 원인이 됩니다.

(2) AIS (선박자동식별시스템)

- 위협 특성 : 암호화되지 않은 개방형 무선 통신을 사용하므로, 데이터 변조를 통해 '유령 선박'을 생성하거나 실제 선박의 신호를 가릴 수 있습니다.
- 사고 영향 : 선박 추적 방해, 충돌 방지 시스템 오류 등을 유발합니다.

(3) ECDIS (전자해도표시정보시스템)

- 위협 특성 : USB 등 외부 매체를 통한 소프트웨어 업데이트 과정에서 악성코드가 유입되기 쉽습니다.
- 사고 영향 : 해도(Chart) 데이터가 변조될 경우, 암초 등의 위험 요소를 인지하지 못해 좌초 사고로 이어집니다.

2. 기관 제어 및 자동화 시스템 (Navigation & Communication)

선박의 '심장'과 '팔다리' 역할을 하는 시스템으로, 직접적인 가동 중단이 목표가 됩니다.

(1) 엔진 및 추진 제어 시스템

- 위협 특성: 원격 유지보수를 위한 통신 채널(Remote Access)이 해킹 통로로 악용됩니다.

- 사고 영향: 엔진 출력 조작 또는 강제 정지를 통해 선박을 통제 불능 상태로 만들며, 항만 내 충돌 사고를 유발할 수 있습니다.

(2) 평형수(Ballast) 제어 시스템

- 위협 특성: 자동화된 밸브 제어 로직을 공격하여 비정상적인 작동을 유도합니다.
- 사고 영향: 선박의 균형을 무너뜨려 전복 위험을 초래하거나 환경 오염 사고를 발생시킵니다.

3. 화물 관리 및 네트워크 시스템 (Cargo & Network)

주로 경제적 갈등이나 해적 활동과 연계된 공격이 이루어집니다.

(1) 로딩 컴퓨터 및 화물 관리 시스템

- 위협 특성: 송장(Invoice) 변조나 화물 적재 데이터 조작 공격이 발생합니다.
- 사고 영향: 위험물 적재 오류로 인한 폭발 사고나, 특정 고가 화물 정보를 해적에게 유출하는 통로가 됩니다.

(2) 선내 공용 네트워크 및 IoT 센서

- 위협 특성: 개인 단말기(BYOD) 연결을 통한 랜섬웨어 감염에 취약하며, 보안이 취약한 저가형 IoT 센서가 전체 네트워크 침투의 통로가 됩니다.
- 사고 영향: 전체 시스템 마비를 통한 운항 지연 및 복구 비용 발생을 초래합니다.

해양 산업 공격 유형

해양 산업에 대한 사이버 공격은 선박의 물리적 통제권을 탈취하려는 직접적 공격과 선박을 둘러싼 생태계 전반을 마비시키는 공급망 공격의 두 가지 축으로 전개되고 있습니다. 특히 선박의 디지털화로 인해 위성통신과 OT 시스템의 접점이 늘어남에 따라, 과거 단순한 정보 탈취에 머물렀던 공격 양상은 이제 실제 운항을 방해하거나 물리적 사고를 유발하는 파괴적인 형태로 진화하고 있습니다.

1. 선박 대상 공격

(1) 위성통신(VSAT) 시스템의 취약성

2025 년 발생한 Lab Dookhtegan 의 이란 선박 공격으로 당시 3 월과 8 월 두 차례에 걸쳐 총 180 척에 달하는 선박의 통신이 마비되었는데, 이는 기본 자격증명 관리 미흡과 구형 펌웨어를 사용하는 시스템의 허점을 파고든 공격이었습니다.

공격자는 공급망을 통해 침투한 뒤 시스템을 파괴함으로써 선박과 육상 간의 연결을 완전히 차단하고 선내 통신망을 마비시키는 파괴력을 보여주었습니다.

(2) GPS/GNSS 스푸핑 공격

2025 년 5 월 홍해에서 발생한 MSC Antonia 호의 좌초 사고를 통해 그 위험성이 극명히 드러났습니다. 이 지역은 현재 하루 1,000 척 이상의 선박이 신호 교란의 영향을 받을 만큼 위협이 일상화되어 있습니다. 인증 체계가 없는 GPS 신호의 특성을 악용해 위조 신호를 전송함으로써, 선박의 항법 장치와 AIS 위치 정보를 왜곡하고 결국 선박을 예정된 경로에서 이탈시켜 물리적 충돌이나 좌초로 몰아넣는 수법을 사용합니다.

(3) OT(운영기술) 시스템에 대한 직접적인 공격

2025 년 12 월 페리 Fantastic 호에서 발견된 RAT(원격제어도구) 설치 사건이 대표적입니다. 이 사고는 승무원이 외부의 지시를 받고 브릿지 워크스테이션에 악성코드가 담긴 USB 를 직접 삽입하며 발생했습니다. 윈도우 XP 와 같은 구형 OS 사용과 네트워크 분리 미흡이라는 취약점을 파고든 이 공격은, ECDIS 해도 데이터를 조작하여 잘못된 정보를 제공하거나 선박의 주요 기관 시스템을 원격으로 제어해 선박의 통제권을 완전히 상실하게 만들 수 있다는 점에서 가장 위협적입니다.

2. 공급망 대상 공격

(1) 조선소 및 기자재 업체 대상

북한 APT 그룹이나 RansomHub 와 같은 조직에 의해 자행되는 핵심 설계 기밀 탈취가 대표적입니다. 이들은 보안이 상대적으로 취약한 협력 업체를 먼저 장악한 뒤 본사인 조선소 네트워크로 침투하여 군함이나 특수선박의 도면을 훔쳐내거나, 생산 라인을 암호화하여 건조 일정을 지연시킵니다. 이는 단순한 금전적 손실을 넘어 국가 해군력의 보안 취약점을 노출하고 국가 전략 자산의 경쟁력을 약화시키는 심각한 결과를 초래합니다.

(2) 항만 운영 시스템(TOS)에 대한 공격

유럽과 북미의 주요 거점 항만에서 발생한 대규모 랜섬웨어 감염 사례를 통해 입증되었습니다. 핵티비스트나 범죄 조직이 항만의 하역 시스템과 물류 데이터를 마비시키면, 컨테이너 처리가 전면 중단되어 인근 해역의 유조선과 화물선이 무기한 대기하게 됩니다.

이러한 공격은 단일 항만의 피해를 넘어 글로벌 공급망에 병목 현상을 일으키고 유가 및 물가 상승 등 전 세계 경제에 즉각적인 혼란을 야기합니다.

(3) SW 및 통신 서비스 공급사를 통한 공격

업데이트 서버나 관리 도구에 악성코드를 심는 방식으로 전개됩니다. 이는 한 번의 침투만으로 해당 소프트웨어를 사용하는 전 세계 수만 척의 선박에 동시에 악성코드를 유포할 수 있다는 점에서 가장 파급력이 큽니다.

특히 선박의 자율운항 기술이나 원격 유지보수 기능이 강화될수록, 신뢰할 수 있는 업데이트 경로가 역설적으로 가장 위험한 공격 통로가 되어 다수의 기관과 선박에 연쇄적인 피해를 입히고 있습니다.

공격 사례 - 선박

2025 년 발생한 Lab Dookhtegan 의 공격은 선박의 위성통신(VSAT) 시스템과 공급망이 얼마나 취약할 수 있는지 보여주는 대표적인 사례입니다. 특정 국가의 해상 물류망을 조직적으로 타격하기 위해 정치적 상황과 사이버 공격을 결합한 고도의 지능형 공격 양상을 보였습니다

File photo of Iranian oil tanker 'Iran Ocean' operated By the National Iranian Tanker Company (NITC)

1 차 공격: VSAT 시스템 침투를 통한 실시간 통신 차단 (2025 년 3 월)

- **피해 규모 및 대상:**
  이란 국영 유조선 회사(NITC) 소속 50 척과 국영 해운(IRISL) 소속 66 척 등 총 116 척이 동시다발적으로 타격받았습니다.

- **공격 주체 및 배경:**
  이스라엘과 연계된 것으로 추정되는 해킹 그룹 'Lab Dookhtegan'은 공격 성공 후 "이란의 해상 테러 및 밀수 활동을 억제하기 위함"이라고 주장했습니다. 특히 미국의 후티 반군 공습 등 지역 내 군사적 긴장이 최고조에 달한 시점에 맞춰 실행되었습니다.

- **기술적 공격 경로 (The Falcon Breach):**
  선박 위성통신 관리 소프트웨어인 'Falcon'의 취약점을 공략했습니다. 공격자는 관리자 권한을 탈취하여 전 세계에 흩어져 있는 116 척 선박의 통신 설정을 한꺼번에 변경하거나 파괴했습니다.

- **피해 상세 내용:**
  통신 암전(Blackout): 선박과 육상 관제소 간의 이메일, 전화, 데이터 전송이 완전히 끊겼습니다.

- **위치 추적 불가:**
  선박의 실시간 위치를 파악하는 시스템이 마비되어 운영사가 자국 선대의 행방을 알 수 없는 위험 상황에 노출되었습니다.

- **운항 지연:**
  항만 입항 시 필요한 사전 교신이 불가능해지면서 선박들이 인근 해상에서 무기한 대기하는 등 막대한 물류 차질이 발생했습니다.

- **시사점:**
  이 사건은 단일 소프트웨어의 취약점이 국가 전체 선단의 운항을 일시에 멈출 수 있다는 '단일 장애점(Single Point of Failure)'의 위험성을 전 세계 해양 산업계에 경고한 사례로 평가받습니다.

2 차 공격: 공급망 인프라 장악을 통한 대규모 선단 사보타주 (2025 년 8 월)

2 차 공격은 1 차 공격에서 미처 확인되지 않았던 공격의 실체를 명확히 드러냈습니다. 단순한 모뎀 수준의 해킹이 아니라, 이란의 핵심 IT·통신 지주사인 'Fanava Group'의 데이터 센터와 허브 인프라 자체를 침투 경로로 활용한 것이 핵심입니다.

- **피해 규모 및 대상:**
  1 차 공격의 연장선상에서 국영 유조선(NITC) 39 척과 화물선(IRISL) 25 척 등 총 64 척이 직접적인 파괴 활동의 표적이 되었습니다.

- **공격 경로 (Provider-level Compromise):**
  공격자는 위성통신 공급사인 Fanava 의 중앙 인프라에 침투하여 약 5 개월간 잠복하며 정보를 수집했습니다. 이를 통해 개별 선박에 일일이 접속할 필요 없이, 중앙 허브에서 수십 척의 선박 시스템에 동시에 접근할 수 있는 루트(Root) 권한을 획득했습니다.

[Part.2]

- **피해 상세 내용 및 파괴 기술:**
  - 데이터 완전 삭제 (Sabotage): 리눅스 기반의 선박 터미널 시스템에서 dd 명령어를 사용하여 6 개의 스토리지 파티션을 강제로 삭제했습니다. 이는 단순한 장애를 넘어 장비를 물리적으로 교체해야 할 정도의 치명적인 손상을 입혔습니다.
  - Falcon 프로세스 강제 종료: 선박 통신의 핵심 소프트웨어인 'Falcon'을 무력화하여 선박과 육상 간의 모든 연결(VOIP, 데이터 전송 등)을 차단했습니다.
  - 기밀 데이터 유출: 내부 네트워크 도표, 운영 체크리스트, 선단 운영 문서를 탈취하여 공개했습니다. 특히 반다르아바스 항구 주변의 실시간 AIS 추적 데이터를 장악함으로써 이란 선단의 모든 움직임을 감시했습니다.

- **시사점:**

  이 공격은 단순한 첩보 활동(Espionage)이 아닌 국가 물류망을 마비시키려는 명백한 '사보타주(Sabotage)'였습니다. 서비스 공급사가 '단일 실패점(Single Point of Failure)'이 될 경우, 국가 전체 선단이 한꺼번에 무력화될 수 있음을 증명했습니다.

공격 사례 - 기자재

FURUNO Electric 랜섬웨어 감염 (2025)

2025 년 10 월, 세계 최대의 해양 전자장비 제조업체 중 하나인 일본의 FURUNO Electric 이 랜섬웨어 공격을 받았습니다. 이 사건은 개별 선박을 직접 해킹하지 않더라도, 장비를 공급하는 원천 업체를 공격함으로써 전 세계 해양 안전 인프라에 광범위한 불확실성을 초래할 수 있음을 입증했습니다.

- **피해 규모 및 대상:**
  레이더(Radar), ECDIS(전자해독장치), VDR(선박운행기록장치) 등 선박 항해의 핵심 기자재를 생산하는 FURUNO 의 일본 본사 및 글로벌 네트워크 시스템이 타격을 입었습니다.

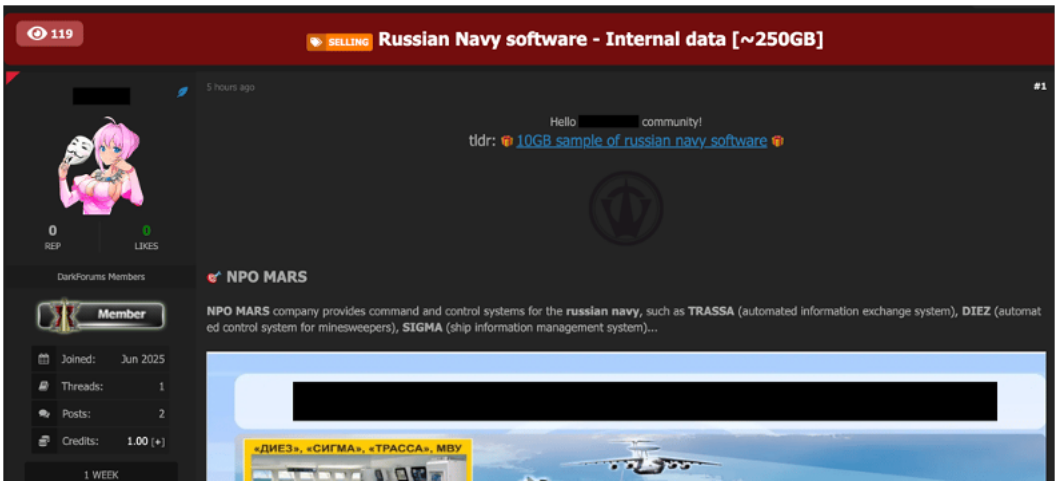
- **공격 주체:**
  신흥 랜섬웨어 조직인 'Rhysida' 그룹으로 밝혀졌으며, 이들은 주로 정부 기관이나 핵심 제조 인프라를 타겟으로 삼는 것으로 알려져 있습니다.

- **공격 방식 (Double Extortion):**
  - 이중 협박: 시스템 내 데이터를 암호화하여 업무를 마비시키는 동시에, 중요 내부 데이터를 미리 탈취하여 이를 다크웹에 공개하겠다고 협박하는 방식을 사용했습니다. 기업의 백업 시스템까지 무력화하여 복구를 어렵게 만들고 금전을 갈취하는 고전적이면서도 치명적인 랜섬웨어 수법입니다.

- **피해 상세 내용 및 영향:**
  - 공급망 위협: FURUNO 의 장비는 전 세계 수많은 선박에 탑재되어 있습니다. 제조사의 시스템 마비는 장비 유지보수, 긴급 소프트웨어 업데이트, 신규 부품 공급의 중단을 의미하며 이는 곧 전 세계 선단의 항해 안전 공백으로 이어집니다.
  - 설계 데이터 유출 우려: 탈취된 데이터에 항해 장비의 설계 도면이나 소스 코드가 포함되었을 경우, 향후 해당 장비를 사용하는 선박들을 대상으로 한 2 차 제로데이(Zero-day) 공격의 발판이 될 수 있다는 점에서 심각성이 큽니다.

공격 사례 - 기자재

러시아 NPO Mars 방산 데이터 유출 (2025)



Attackers' post on a data leak forum. Image by Cybernews.

2025 년 7 월, 러시아 해군의 핵심 전투 지휘 시스템을 개발하는 방산업체 NPO Mars 의 내부 데이터가 다크웹에 노출되었습니다. 이 사건은 군함의 건조를 넘어, 함정의 '두뇌'인 지휘통제 시스템의 설계도가 유출되었을 때 발생하는 안보적 파장을 극명하게 보여줍니다.

- **피해 규모 및 대상:**
  러시아 해군의 자동화 지휘통제 시스템을 설계하는 NPO Mars 의 서버에서 약 250GB 규모의 기밀 데이터가 탈취되었습니다.

- **공격 주체:**
  구체적인 공격 그룹의 정체는 밝혀지지 않았으나, 탈취된 데이터가 다크웹 포럼에 전격 공개되면서 세상에 알려졌습니다.

- **피해 상세 내용 및 유출 자산:**
  - SIGMA 전투정보시스템: 러시아 해군 함정의 핵심 지휘통제 체계인 'SIGMA' 관련 데이터가 유출되었습니다. 이는 함정의 무장 운용 및 전술 판단 로직이 적대 세력에게 노출되었음을 의미합니다.

- DIEZ 소해정 제어시스템: 기뢰를 제거하는 소해정의 자동 제어 시스템 관련 기술 정보가 포함되었습니다.
- 기술 매뉴얼 및 도면:
  시스템의 작동 원리, 네트워크 구조, 하드웨어 사양이 담긴 상세 매뉴얼이 유출되어 시스템의 취약점을 분석할 수 있는 토대가 마련되었습니다.

- 영향 (Strategic Impact):
  - 지휘통제 무력화: 전술 네트워크의 구조가 노출됨에 따라, 실제 교전 상황에서 적대국이 러시아 해군의 통신을 감청하거나 가짜 명령을 삽입하는 등의 전자전 공격에 매우 취약해졌습니다.
  - 비대칭 전력 손실: 소해 시스템의 정보 유출은 기뢰를 이용한 봉쇄 작전 시 러시아 해군의 대응 능력을 미리 예측하고 차단할 수 있게 만들어, 해상 통제권에 심각한 위협을 가합니다.

공격 사례 - 조선소

Sevmash 조선소 및 핵잠수함 기밀 탈취 (2025)

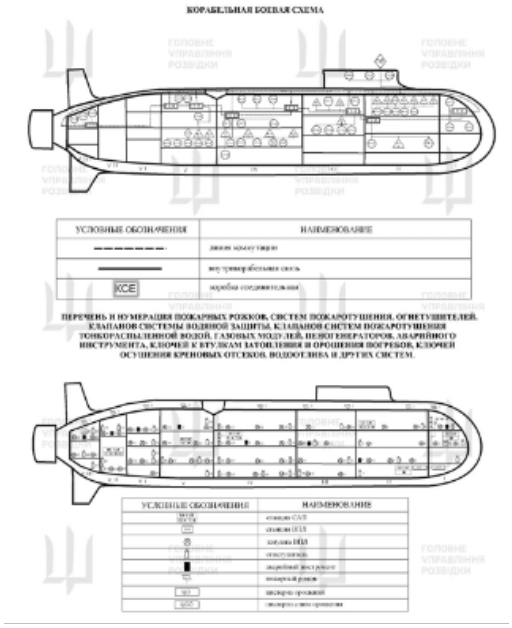

КОРАБЕЛЬНАЯ БОЕВАЯ СХЕМА
УСЛОВНЫЕ ОБОЗНАЧЕНИЯ
НАИМЕНОВАНИЕ
ПЕРЕЧЕНЬ И НУМЕРАЦИЯ ПОЖАРНЫХ РОЖКОВ, СИСТЕМ ПОЖАРОТУШЕНИЯ, ОГНЕТУШИТЕЛЕЙ, КЛАПАНОВ СИСТЕМЫ ВОДЯНОЙ ЗАЩИТЫ, КЛАПАНОВ СИСТЕМ ПОЖАРОТУШЕНИЯ ТОНКОРАСПЫЛЕННОЙ ВОДОЙ, ГАЗОВЫХ МЕДУЗЕЙ, ПЕЧЕЙ-ИЗВЕРАТОРОВ, АВАРИЙНОГО ИНСТРУМЕНТА, КЛЮЧЕЙ К КРУГЛЫМ ЗАТОЛЕНИЯМ И ОРОШЕНИЯ ПОГРЕБОВ, КЛЮЧЕЙ ОСУШЕНИЯ КРЕНОВЫХ ОТСЕКОВ, ВОДОТЕЛИВА И ДРУГИХ СИСТЕМ.
УСЛОВНЫЕ ОБОЗНАЧЕНИЯ
НАИМЕНОВАНИЕ

Diagram of Russian submarine posted by HUR.

2025 년 8 월, 러시아의 핵심 군사 시설인 Sevmash 조선소가 우크라이나 국방정보총국(HUR)의 사이버 공격을 받았습니다. 이 공격은 러시아의 최신형 Borei-A 급 핵잠수함인 'Knyaz Pozharsky' 호의 핵심 정보를 정밀 타격했다는 점에서 군사적 파급력이 매우 컸던 사건입니다.

- **피해 규모 및 대상:**
  러시아 북부 세베로드빈스크에 위치한 Sevmash 조선소의 서버가 해킹되어, 건조 중인 핵잠수함과 관련된 방대한 양의 기밀 데이터가 유출되었습니다.

- **공격 주체:**
  우크라이나 국방정보총국(HUR) 산하의 사이버 부대로 확인되었으며, 전시 상황에서 적국의 핵심 전략 자산을 무력화하기 위한 목적으로 수행되었습니다.

[Part.2]

- **피해 상세 내용 및 유출 정보:**
  물리적 취약점 노출: 잠수함의 수밀구획 도면과 기술적 취약점 정보가 유출되었습니다. 이는 잠수함의 어느 부위를 타격해야 침몰시킬 수 있는지에 대한 '급소' 정보가 적국에게 넘어갔음을 의미합니다.

- **인적 자원 정보:**
  승조원 66 명의 이름, 계급뿐만 아니라 체력 점수와 의료 평가 등 극히 개인적인 정보까지 탈취되었습니다. 이는 향후 승조원을 대상으로 한 개별적인 포섭이나 심리전의 자료로 악용될 수 있습니다.

- **운영 기밀:**
  전투 매뉴얼과 운영 일정, 설계도면이 통째로 유출되어, 해당 핵잠수함의 작전 능력과 항로 패턴을 미리 예측할 수 있게 되었습니다.

- **영향 (Strategic Impact):**
  - 핵 억제력 약화: 러시아의 3 대 핵전력 중 하나인 Borei-A 급 핵잠수함의 보안이 무너짐으로써, 러시아의 해상 핵 보복 능력이 심각한 불확실성에 직면하게 되었습니다.
  - 심리적 위축: 국가 최상위 보안 시설인 핵잠수함 조선소가 뚫렸다는 사실만으로도 군 내부의 사기와 보안 체계에 대한 신뢰에 치명적인 타격을 입혔습니다.

공격 사례 - 항만

파라과이 Terport 터미널 랜섬웨어 감염 (2025)

2025 년 12 월, 파라과이의 주요 터미널 운영사인 Terport 가 랜섬웨어 공격을 받았습니다. 항만 터미널 운영 시스템(TOS)은 선박의 입출항, 컨테이너 하역 및 적재 등을 관리하는 핵심 인프라이기에, 이를 볼모로 잡는 공격은 매우 높은 경제적 타격을 목표로 합니다.

- **피해 규모 및 대상:**
  파라과이의 물류 요충지를 담당하는 Terport 터미널의 운영 데이터베이스 및 관리 네트워크가 타격을 입었습니다.

- **공격 주체:**
  신흥 사이버 범죄 조직인 'LYNX' 랜섬웨어 그룹으로 확인되었습니다. 이들은 주로 대규모 물류나 제조 인프라를 공격하여 고액의 몸값을 요구하는 특성을 보입니다.

- **공격 방식 (Data Exfiltration & Ransom):**
  - 시스템 침투 및 탈취: 운영 네트워크에 침투하여 내부 데이터를 먼저 탈취한 뒤, 시스템 전체를 암호화하는 방식을 취했습니다.
  - 이중 협박: 데이터를 복구해 주는 조건과 더불어, 탈취한 기밀 정보를 외부에 공개하지 않는 대가로 금전을 요구하는 전형적인 이중 협박 전술을 구사했습니다.

- **피해 상세 내용:**
  - 물류 기록 및 운영 데이터: 선박의 스케줄, 화물 적재 목록, 컨테이너 위치 정보 등 항만 운영에 필수적인 실시간 데이터가 유출 및 암호화되었습니다.
  - 파트너 및 고객 정보: 터미널을 이용하는 선사, 화주, 물류 파트너들의 민감한 비즈니스 정보가 유출되어 2 차 피해 우려를 낳았습니다.

- **영향 (Logistics Disruption):**
  - 하역 작업 중단: 시스템 마비로 인해 수동으로 작업을 전환해야 했으며, 이는 컨테이너 처리 속도를 급격히 저하시켜 항만 정체 현상을 유발했습니다.
  - 공급망 신뢰도 하락: 국가 주요 물류 거점의 보안 취약점이 노출되면서, 글로벌 선사들의 기항지 신뢰도에 부정적인 영향을 미쳤습니다.

공격 사례 - 항만

벨기에 안트베르펜-제브뤼허 항만 마비 (2025)

2025 년 상반기, 유럽에서 두 번째로 큰 규모를 자랑하는 벨기에의 안트베르펜-제브뤼허 항만이 국가 지원 해커 그룹의 집중적인 공격을 받았습니다. 이 사건은 단순한 금전 갈취를 넘어, 지정학적 갈등 상황에서 항만이 어떻게 전략적 타격 목표가 될 수 있는지를 여실히 보여주었습니다.

- **피해 시점:**
  2025 년 상반기

- **공격자:**
  러시아 배후의 국가 지원 해커 그룹인 APT28 (Fancy Bear) 및 연계 핵티비스트 조직

- **피해 대상:**
  벨기에 안트베르펜-제브뤼허 항만 운영 시스템 및 유관 물류 네트워크

- **공격 방식:**
  분산 서비스 거부(DDoS) 공격 및 시스템 침투로 항만 운영의 핵심인 터미널 운영 시스템(TOS)에 대규모 트래픽을 발생시켜 마비시켰습니다. 동시에 내부 네트워크에 침투하여 물류 데이터와 운영 기밀을 탈취하는 복합 공격을 수행했습니다.

- **피해 내용:**
  - 운영 시스템 중단: 선박의 입출항 관리와 컨테이너 하역 스케줄링 시스템이 일시적으로 중단되었습니다.
  - 물류 정체: 자동화된 하역 장비와 게이트 시스템이 먹통이 되면서 항만 인근에 수천 대의 트럭과 수십 척의 선박이 대기하는 물류 대란이 발생했습니다.

- **영향 (Strategic Disruption):**
  - 공급망 무력화: 유럽 내 에너지 및 물자 수송의 핵심 관문이 막히면서, 인근 국가들의 산업 생산에 연쇄적인 차질을 빚었습니다.
  - 지정학적 압박: 우크라이나를 지원하는 서방 국가들에 대한 보복성 공격으로 해석되며, 사이버 공격이 해상 물류를 볼모로 한 강력한 비대칭 무기가 될 수 있음을 증명했습니다.

2026 년 해양 사이버위험 리스크 예상

[AI Sabotage] AI 에이전트 기반 자율형 공격의 고착화

2026 년은 AI 가 공격의 보조 도구를 넘어 스스로 작전을 수행하는 '자율형 공격'의 시대가 될 것입니다. 2025 년 중국 국가지원 그룹(GTG-1002)이 보여준 사례처럼, AI 에이전트는 취약점 분석부터 데이터 유출까지 공격 과정의 90%를 인간의 개입 없이 자율적으로 수행합니다. 이는 사이버 공격의 진입 장벽을 낮추어 저숙련 공격자도 국가 수준의 정교한 공격을 대규모로 감행할 수 있게 만들며, 해양 기관들을 대상으로 한 공격 빈도를 폭발적으로 증가시킬 전망입니다.

[Supply Chain Pivot] 공급망 상위 노드 장악 및 연쇄 감염

단일 선박을 공격하는 대신 통신사, OEM 기자재 업체 등 공급망의 '길목'을 노리는 공격이 주류를 이룰 것입니다. Lab Dookhtegan 사례와 같이 단일 위성통신 공급사 침투만으로 전체 선대를 마비시키는 전술이 보편화되며, 특히 CISA 등 주요 보안 기관이 경고한 중국산 해양 장비의 원격 접속 취약점을 악용하려는 시도가 늘어날 것입니다. 이는 기자재 업체의 유지보수 채널이 다수 선박을 동시에 감염시키는 '피벗(Pivot)' 포인트가 될 수 있음을 시사합니다.

[C2 Manipulation] 지휘통제(C2) 조작과 물리적 타격의 결합

사이버 공격이 물리적 파괴로 이어지는 '사이버-물리 결합 공격'이 더욱 정교해질 것입니다. 분쟁 지역에서의 GPS 재밍과 스푸핑은 일상화될 것이며, 특히 해커 그룹이 해상 지휘통제(C2) 시스템이나 AIS 데이터를 탈취하여 이를 실제 미사일 공격의 좌표 설정에 활용하는 사례가 빈번해질 것으로 보입니다. 이는 사이버 보안이 곧 선원의 생명과 선박의 생존권과 직결되는 물리적 보안임을 의미합니다.

[Ransomware Cartel] 핵티비즘과 랜섬웨어 카르텔의 연대

정치적 목적을 가진 핵티비스트와 금전적 이득을 노리는 랜섬웨어 조직 간의 '카르텔화'가 심화될 것입니다. 캄보디아-태국 분쟁 사례에서 보듯, 분쟁 국가의 핵티비스트들이 랜섬웨어 그룹의 공격 인프라(RaaS)를 빌려 상대국의 항만이나 물류 시스템을 무차별 타격하는 양상이 두드러질 것입니다. 이들은 이중·삼중 협박 전술을 보편화하고 백업 시스템까지 정밀 타격하여 평균 요구액 수백만 달러 규모의 고부가가치 공격에 집중할 전망입니다.

[Regulatory Pressure] 강화된 국제 보안 규제와 자격 리스크

2026 년에는 기술적 위협뿐만 아니라 규제 준수 여부가 해양 기업의 생존을 결정하는 리스크로 작용할 것입니다. IACS UR E26/27 과 같은 강력한 사이버 복원력 요구사항이 전면 적용됨에 따라, 보안 인증을 갖추지 못한 선박이나 기자재 업체는 운항 자격 상실이나 기항 거부와 같은 실질적인 운영 리스크에 직면하게 됩니다. 또한 Shadow Fleet 와 같이 규제를 회피하는 선단이 보안 취약점의 사각지대로 남으면서, 이를 차단하려는 국제 사회의 압박과 사이버 제재가 동시에 강화될 것입니다.

대응방안

운항선 및 선사, 공급망의 MCTI 기반 선제적 보안 체계 구축

단순한 사후 방어 위주에서 벗어나 해양 사이버 위협 인텔리전스(MCTI: Maritime Cyber Threat Intelligence)를 활용한 능동적 방어 체계를 구축해야 합니다. 전 세계 해역에서 발생하는 GPS 스푸핑, 특정 선사 타겟 랜섬웨어, 위성통신 취약점 정보를 실시간으로 수집하고 분석하는 것이 핵심입니다. 이를 선박 보안관제센터(SOC)와 실시간으로 공유하여 공격이 발생하기 전 취약 패치를 완료하거나 위험 해역 진입 시 강화된 감시 태세를 가동함으로써 정보의 사각지대에 놓인 선박이 예방적 방어를 수행할 수 있도록 지원해야 합니다.

신조선 및 현존선 위협 모델링 기반 위협 예측 및 개선

선박의 설계부터 실제 운항 단계까지 전 수명 주기에 걸쳐 위협 모델링(Threat Modeling)을 적용하는 체계가 필요합니다. 선박 내 OT 와 IT 자산을 명확히 식별한 후 데이터의 흐름과 공격 경로를 가상으로 시뮬레이션해야 합니다. 특히 자율운항 시스템이나 원격 유지보수 채널처럼 외부 접점이 많은 핵심 자산에 대해 공격 시나리오를 사전에 정의하고, 이를 바탕으로 설계 변경이나 네트워크 격리 등의 개선책을 운항 현장에 즉각 반영함으로써 잠재적 위험을 선제적으로 제거해야 합니다.

신조선 및 현존선 보안 테스팅 정례화

시스템 구축 이후에도 보안 수준을 유지하기 위해 실제 침투 상황을 가정한 보안 테스팅을 정기적으로 실시해야 합니다. 신조선의 경우 인도 전 모의해킹을 의무화하여 초기 보안성을 검증하고, 운항 중인 현존선은 최소 연 1 회 이상의 취약점 스캐닝과 위성통신 보안 점검을 수행해야 합니다. 특히 승무원의 실수나 외부 저장매체 유입과 같은 인적 보안 취약점까지 포함한 실습형 테스트를 병행하여 신종 공격 기법에 대한 선박의 복원력을 상시 유지하는 것이 중요합니다.

선사 및 조선소의 CSMS 구축

기술적인 방어를 넘어 기업 전체의 보안 거버넌스를 체계적으로 관리하는 사이버 보안 관리 시스템(CSMS: Cyber Security Management System) 구축이 필수적입니다. ISO/IEC 27001 이나 NIST 프레임워크를 기반으로 해양 산업에 특화된 보안 프로세스를 수립해야 합니다. 조선소는 핵심 설계 도면 보호와 건조 공정 내 운영기술 보안에 집중하고, 선사는 선단 전체의 원격 관제 및 사고 대응 프로토콜을 포함하는 관리 체계를 갖추어 글로벌 시장이 요구하는 높은 수준의 보안 신뢰도를 확보해야 합니다.

기자재의 CSMS 구축 및 공급망 보안 강화

선박에 탑재되는 모든 소프트웨어와 하드웨어는 보안이 검증된 상태로 공급되어야 합니다. 기자재 업체는 제품 개발의 전 과정에 보안을 내재화하고, 소프트웨어 구성 명세서(SBOM)를 제공하여 취약점 발생 시 즉각적인 식별과 조치가 가능하도록 지원해야 합니다. 특히 국제선급연합회(IACS)의 UR E27 규정을 준수하여 장비 자체의 보안 기능을 표준화함으로써, 공급망의 하위 단계에서 발생한 취약점이 선박 전체의 위협으로 전이되는 것을 원천적으로 차단해야 합니다.

사이버 신뢰와 회복 탄력성을 향한 여정: 규제 준수를 넘어 실전 검증으로

2025 년 해양 사이버 사고 건수가 전년 대비 103% 급증했다는 데이터는 우리에게 명확한 메시지를 던지고 있습니다. 이제 사이버 보안은 단순히 사고를 막는 기술적 영역을 넘어, 스마트 선박의 안전 운항과 비즈니스 연속성을 보장하는 핵심 경쟁력이 되었습니다.

과거 고립되었던 선상 제어 시스템(OT)이 위성 통신을 통해 육상 네트워크와 긴밀히 연결되면서 공격 표면은 전례 없이 확장되었습니다. 2025 년 발생한 위성통신 인프라 사보타주와 핵잠수함 설계도 유출 사례에서 보듯, 한 번의 침투는 국가 전략 자산의 보안 취약점을 노출하고 글로벌 공급망 전체에 심각한 병목 현상을 야기할 수 있습니다.

특히 다가오는 2026 년은 단순한 위협의 증가를 넘어선 중대한 변곡점이 될 것입니다. 2024 년 7 월 IACS UR E26/27 규제 발효 이후 계약된 선박들이 본격적으로 인도되는 올해는, 사이버 보안이 도면상의 계획을 넘어 실제 선박의 '운항권(License to Sail)'을 결정짓는 실전 검증의 원년입니다.2026 년은 AI 기반의 자율형 공격과 공급망 상위 노드를 노리는 정교한 위협이 일상화될 것입니다. 이에 대응하기 위해 우리는 다음과 같은 변화를 수용해야 합니다.

- **인텔리전스 기반의 선제적 방어:**
  범용 CTI 의 한계를 넘어 NMEA, AIS 등 해상 고유 프로토콜과 다크웹 징후를 이해하는 해양 특화 인텔리전스를 확보해야 합니다.
- **보안의 내재화(Secure by Design):**
  설계 단계부터 위협 모델링을 적용하고, IACS UR E26/27 등 강화되는 국제 규제에 선제적으로 대응하는 관리 체계(CSMS)를 구축해야 합니다.
- **사이버 회복탄력성(Cyber Resilience):**
  위협과 공격을 받더라도 필수 기능을 유지하며 신속하게 복구할 수 있는 회복 역량에 집중해야합니다. 이를 위해조선소, 선사, 기자재 업체가 협력적 거버넌스를 구축하여 소프트웨어 구성 명세서(SBOM)를 공유하고 위협 정보를 공동 대응하는 유기적인 보안 생태계를 조성해야 합니다.

정보가 부족한 해양 보안 분야에서 본 백서가 막연한 불안감을 확신으로 바꾸는 이정표가 되기를 바랍니다. 싸이터는 앞으로도 해양의 언어를 이해하는 전문적인 인텔리전스를 통해, 디지털 대전환의 파도를 맞이한 해양 산업에 사이버 신뢰와 회복 탄력성을 제공하는 든든한 파수꾼이 될 것을 약속드립니다.

주요 해양 사이버보안 용어 정리

백서 본문에서 다루는 핵심 기술 및 규제 용어들을 독자들이 쉽게 이해할 수 있도록 정의했습니다.

- **OT (Operational Technology, 운영기술):**
  선박의 엔진 제어(IAS), 평형수 관리(BWMS) 등 물리적 장치를 제어하고 모니터링하는 기술입니다.

- **MCTI (Maritime Cyber Threat Intelligence):**
  해상 프로토콜(NMEA, AIS 등)과 해양 산업 특유의 공격 전술을 분석하여 제공하는 해양 특화 위협 인텔리전스입니다.

- **GPS Spoofing/Jamming:**
  허위 위성 신호를 송출하여 위치 정보를 왜곡하거나(스푸핑), 강력한 방해 전파로 신호 수신을 차단하는(재밍) 공격입니다.

- **IACS UR E26/E27:**
  국제선급연합회에서 제정한 공통 규칙으로, 선박(E26)과 기자재(E27)의 사이버 복원력 확보를 위한 필수 요구사항입니다.

- **CSMS (Cyber Security Management System):**
  조직의 자산과 시스템을 보호하기 위해 수립된 체계적인 사이버 보안 관리 시스템입니다.

- **VSAT (Very Small Aperture Terminal):**
  선박에서 사용하는 위성통신 시스템으로, 육상과의 데이터 송수신 및 선내 네트워크 연결의 핵심 통로입니다.

- **ECDIS (Electronic Chart Display and Information System):**
  종이 해도 대신 디지털 해도를 표시하고 항해 정보를 통합 관리하는 전자해도 정보시스템입니다.

- **AIS (Automatic Identification System):**
  선박의 위치, 침로, 속력 등 항행 정보를 타선 및 육상 관제소와 자동으로 교환하는 장치입니다.

해양 기업을 위한 사이버보안 자가 진단 체크리스트

선사, 조선소, 기자재 업체 관리자가 현재의 보안 수준을 점검하고 대응 방안을 수립하는 데 활용할 수 있습니다.

점검 영역	점검 항목 (Checklist)	결과 (V)
정책 및 관리	국제 해양 보안 표준(IMO, IACS 등)을 준수하는 CSMS 체계를 보유하고 있는가?	
위협 모니터링	해양 특화 위협(MCTI)을 실시간으로 수집하고 분석할 수 있는 체계가 있는가?	
자산 및 설계	선박 IT/OT 자산에 대한 위협 모델링을 통해 공격 경로를 파악하고 있는가?	
공급망 보안	주요 기자재에 대해 SBOM을 확보하고 공급사의 보안성을 검증하고 있는가?	
사고 대응	VSAT 차단이나 시스템 마비 시 시나리오별 비상 대응 절차를 갖추고 있는가?	
정기 테스팅	연 1회 이상 신조선 및 현존선 대상 모의해킹 등 보안 테스트를 실시하는가?	
인적 보안	승무원을 대상으로 한 USB 사용 금지 및 피싱 메일 대응 훈련을 실시하는가?	

CONTACT US

본 백서에서 다룬 2025 년 해양 사이버 위협 분석 및 2026 년 리스크 전망에 대해 보다 상세한 정보가 필요하시거나, 해양 산업 전반의 사이버 보안 전략 수립에 관한 기술적 자문이 필요하시면 언제든 아래의 채널로 연락해 주시기 바랍니다.

싸이터(CYTUR)는 선박의 설계 단계부터 운용 단계에 이르는 전 과정에 걸쳐 'Secure by Design' 철학을 실현하며, 고객사의 소중한 해상 자산과 비즈니스 연속성을 보호하기 위한 최적의 파트너가 되어 드릴 것을 약속드립니다.

싸이터(CYTUR) | Cyber Trust & Resilience for Maritime
E-mail: sales@cytur.net
Website: http://cytur.net