KIMS Periscope
For God · For Nation · For Peace

제 211 호 2020 년 10 월 21 일

미래 사이버 위협과 해군 사이버작전 역량 강화방안

지난 2019년 6월, 우리 해군은 국방개혁 2.0에 부합하는 해군 전력을 갖추기 위해 해군 2045를 구현하는 '국방개혁 2.0 해군추진계획' 설계도를 공개하고 △ 전방위 안보위협 대응 △ 첨단 과학기술 기반 정예화 △ 선진화된 국가에 걸맞는 군대를 목표로 해양강군 건설을 위해 노력해오고 있다.

오랜 기간 전부터 해군은 기술환경 변화에 따라 나무에서 강철로, 돛에서 증기로 해군 전력의 핵심기반과 동력을 진화시켜 작전수행 능력을 최적화시켜 왔으며, 이제는 급격하게 변화하고 있는 ICT 기술 발전에 따른 미래전 양상 변화에 선제적·능동적 준비가 필요한 시점에 이르렀다. 특히 스마트십(Smart Ship)의 등장과 선육간 네트워킹 강화로 해킹을 통한 사이버 위협이 군에 치명적인 영향을 미칠 것으로 예측됨에 따라 해군의 사이버위협 대응 능력 확보와 사이버작전 역량 강화를 위한 중·장기적 계획 수립이 절실히 요청된다.

이에 본고는 해양 분야 기술환경 변화에 따른 미래 사이버 위협에 대해 간략히 살펴보고, 해군 사이버작전 역량 강화방안과 구체적 과제에 대해 제언하고자 한다.

고려대 정보보호대학원
교 수
임 종 인

지난 2019년 6월, 우리 해군은 국방개혁 2.0에 부합하는 해군 전력을 갖추기 위해 해군 2045를 구현하는 '국방개혁 2.0 해군추진계획' 설계도를 공개하고 △ 전방위 안보위협 대응 △ 첨단 과학기술 기반 정예화 △ 선진화된 국가에 걸맞는 군대를 목표로 해양강군 건설을 위해 노력해오고 있다.

오랜 기간 전부터 해군은 기술환경 변화에 따라 나무에서 강철로, 돛에서 증기로 해군 전력의 핵심기반과 동력을 진화시켜 작전수행 능력을 최적화시켜 왔으며, 이제는 급격하게 변화하고 있는 ICT 기술 발전에 따른 미래전 양상 변화에 선제적·능동적 준비가 필요한 시점에 이르렀다. 특히 스마트십(Smart Ship)의 등장과 선육간 네트워킹 강화로 해킹을 통한 사이버 위협이 군에 치명적인 영향을 미칠 것으로 예측됨에 따라 해군의 사이버위협 대응 능력 확보와 사이버작전 역량 강화를 위한 중·장기적 계획 수립이 절실히 요청된다.

이에 본고는 해양 분야 기술환경 변화에 따른 미래 사이버 위협에 대해 간략히 살펴보고, 해군 사이버작전 역량 강화방안과 구체적 과제에 대해 제언하고자 한다.

스마트 해군이 직면할 新사이버 위협

우리 해군이 건설하고자 하는 스마트 해군(SMART Navy)은 스마트 전투함정(SMART Battleship), 스마트 작전운용(SMART Operation), 스마트 협력(SMART Cooperation)을 기반으로 미래전에 능동적으로 대응할 수 있는 해양 강군으로의 혁신적 전환을 목표로 한다. 4차 산업혁명 첨단 기술의 적용과 해양 무인체계의 구축을 위해서는 선박에 IT(Information technology)/OT(Operational Technology) 장비 탑재가 필수적이며 이는 다양한 센서 통신의 기하급수적인 증가와 기존 폐쇄형 환경(Closed or Proprietary)에서 개방형 체계(Open Architecture)으로의 전환을 전제로 한다. 더불어 선내 와이파이 및 5G 통신이 확대될 것이며, 통신 채널도 정보공유를 위한 단방향 위주의 위성통신에서 제어가 가능한 양방향 네트워크로 전환될 것으로 예측된다.

이러한 해군 전력체계의 변화에 따라 사이버 공격의 대상과 범위가 대폭 확대될 것이며, 머지않아 기존에 없던 새로운 차원의 사이버 위협이 필연적으로 발생할 것이다. 이미 '17년 영·미안보정보협의회(BASIC : British American Security Information Council)는 핵잠수함을 포함한 많은 진보된 무기체계들이 너무 많은 컴퓨터시스템에 의존하고 있음을 지적하며 관련 취약점을 통해 영국 핵잠수함에 탑재된 '트라이던트 미사일'이 해커의 공격으로 무력화될 수 있음을 경고한 바 있으며, '17년 연이어 발생한 미 해군 이지스함 충돌 사고 또한 중국의 사이버 공격에 의해 발생하였을 가능성이 지속적으로 제기되고 있다. 우리 군의 경우 한국형 미사일방어체제(KAMD)의 핵심적인 역할을 하는 조기경보위성, 레이더, 이지스함 등이 Link-16에 대한 네트워크 교란 및 체계 호환성 취약점 등을 통해 공격당할 경우 대응 지연 유발 및 미사일 방어 실패 등 심각한 결과를 초래할 가능성이 있다.

우리 해군의 핵심전력인 이지스함은 사이버 공격의 예외가 될 수 있을까? 세종대왕함 설계·생산업체나 전투체계 개발업체가 해킹되어 전투체계 프로그램, 이지스 논리체계 등 알고리즘이 유출되면 적군이 세종대왕함의 스파이 레이더를 무력화하고 오폭을 유도하는 것은 시간문제다. 레이더 없는 이지스함은 단순 병력수송선과 다를 바 없으며, 사이버 위협은 이지스함 건조 비용보다 훨씬 저렴한 비용으로 '신의 방패'라고 불리는 이지스함을 한 순간에 무력화시킬 수 있다.

무기체계 보안 위협과 보안 강화방안

이처럼 복잡한 SW가 결합되어 있는 첨단무기체계에 대한 의존도가 증가하는 미래전에서는 보안 취약점을 이용한 사이버 위협이 군사작전 수행에 큰 영향을 미칠 수 있고, 이를 방호하기 위한 사이버보안의 중요성이 증대될 것으로 예상된다. 이미 국제사회에서는 해킹을 통해 주요 군사자료를 빼내고 유출하여 유사 첨단무기체계 복제 및 무기체계 해킹 목적으로 활용하는 것이 일상적인 첩보·군사 전략으로 활용되고 있다. 이와 관련하여 미국이 오래전부터 군과 정보기관에 사이버무기 개발과 관련하여 공급망 공격 등을 수행할 사이버무기 개발 팀을 두고 공세적 사이버작전과 정보 수집작전을 수행하고 있음은 스노든과 위키리크스 폭로에 의해 널리 알려진 바 있다.

한편 우리 군은 무기체계 보안 위협에 대한 대비체계가 미흡한 실정이다. 무기체계 보안의 기본 원칙과 절차가 제대로 지켜지지 못하고 있을 뿐 아니라 명확한 사이버무기 개발·평가 체계를 갖추지 못하고 있고, 이와 관련한 전문성을 갖춘 인력과 기술도 부족한 것이 현실이다. 미국은 국방수권법 2016(NDAA 2016)과 무기체계 보안 전략을 수립하였고, 美 공군은 무기체계 획득 사이버 캠페인 계획과 무기체계 평가를 전담할 사이버 복원성 전담국(CROWS; Air Force Cyber Resiliency Office for Weapons Systems) 등 전담조직을 두고 있으며, 美 국방성은 무기체계 보안 강화를 위한 종합적인 체계와 방법론을 포함하는 프로그램 보호 계획 가이던스인 DoDI 5000.02를 적용하여 무기체계에 대한 적국의 사이버 위협에 적극적으로 대응하고 있다.

우리 군도 국산/수입 무기체계 SW개발보안에서부터 보안검증과 관리에 이르는 전체 라이프사이클을 책임질 무기체계 SW 통합보안관리 전문기관을 설립하고 방산기술 개발 단계의 보안 설계(Security by Design) 구현 등 공급망 전 단계의 사이버보안을 강화하여 발생 가능한 보안위협을 사전에 제거하기 위해 적극적인 노력을 기울여야 한다. 더불어 내·외부의 보안 위협으로부터 무기체계를 보호하기 위한 군·방산체 등의 기술, 프로세스, 사람에 대한 위험관리 차원의 내부통제 시스템을 구축할 필요가 있다.

해군 내 사이버 병과/주특기 신설 요청

기존 전투무기체계와는 다른 사이버영역이 출현함에 따라 우리 군에도 사이버작전을 전문적으로 수행할 수 있는 병과와 주특기 신설이 필요하다. 군 차원에서 사이버작전에 필요한 일력을 적재적소에 활용하고 각 군의 특성에 맞는 작전을 운용하기 위해서는 사이버작전을 전문적으로 수행할 수 있는 보직을 보장하고 전문성을 지속적으로 향상시킬 수 있는 병과의 신설이 필수적이다.

미국은 이미 10년 전부터 사이버 병과와 주특기의 중요성을 인지하고 육군, 해군, 공군, 해병대에 각각 사이버작전 주특기 마련하여 사이버 공격·방어·지원을 포함한 사이버작전 분야에 명확한 임무와 역할을 부여하고, 전문성을 갖춘 인력을 사이버작전 관련 업무에 배치하고 있다. 미 해군은 암호전 지휘관(181X), 정보 전문가(182X), 사이버전 엔지니어 지휘관(184X) 신설로 장교 위주의 사이버작전 수행 체계를 구축하고 있으며, 지

속적 역량 개발을 위한 다양한 교육 기회를 제공하고 있다. 나아가 미 육군은 지난 '19년 '사이버'를 하나의 독립된 병과로 만들고 보병, 포병, 기갑 등과 나란히 전투병과에 편성하였다.

이처럼 우리 해군도 사이버공간을 육·해·공에 이은 '제4의 전선'으로 취급하고 사이버작전을 해상작전과 동급으로 다뤄야 한다. 이미 우리 육군은 관련 논의를 진전시키어 사이버 위협 대응능력 향상을 위해 '19년 사이버 특기를 신설한 바 있으며, 사이버작전사령부도 장교·부사관의 사이버전문특기를 신설하였다. 해군도 해양 분야의 사이버전 특수성에 대응하기 위해 사이버작전을 전문적으로 수행할 수 있는 사이버 병과나 주특기 신설에 대한 구체적인 논의를 시작해야 할 시점이다.

사이버병과 또는 사이버작전 주특기 신설은 우리 군이 사이버공간을 전략적으로 활용하기 위한 출발점이다. 장기적으로 사이버 전문인력에 대한 체계적인 정책 구상과 교육훈련, 커리어패스 설계를 통해 미래전 대비를 위한 군 인력양성·관리체계의 혁신을 시작해야 한다.

해양 분야 미래전 양상 변화에 따른 사이버보안 패러다임의 전환 필요성

우리 해군이 목표로 하는 스마트 해군(SMART Navy)은 대부분의 함정이 첨단 ICT를 탑재하고, 수중·해상·공중 전장 정보가 실시간으로 공유되며, 다양한 탑재 장비가 하나의 통합서버체계로 구축되어 관리된다. 이는 네트워크 중심 작전, 신속결정 작전, 전장 공간의 확대 등 미래전 양상을 완전히 새로운 형태로 변화시킬 것이다.

이러한 관점에서 사이버작전은 단순히 사이버보안 차원에 한정하여 다뤄져서는 안되며 임무 보안, 작전 보안의 차원에서 다뤄져야 한다. 특히 자연환경의 영향을 많이 받고 시스템의 물리적 환경 여건의 변동성이 높아 평시에도 시스템의 가용성(Availability)이 최우선시되는 해양 부문에서는 사이버 위협에 대비하여 회복탄력성(Resilience)[1] 관점에서

[1] 사이버 회복탄력성(Cyber Resillence)란 "사이버공격 또는 IT 시스템에 악영향을 주는 어떠한 이벤트가 발생했을 경우, IT 시스템을 지속적으로 운영할 수 있는 대응능력"을 의미하며, 사이버 공격 위험 저하 및 조직 보호를 목표로 하는 사이버 보안과는 달리 주된 목표를 비즈니스 요구사항 및 연속성 유지에 두고 있어 목

복구 및 임무 연속성이 보장되도록 하는 것이 중요하다. 사이버 침해를 원천적으로 막는 것을 목표로 하는 기존의 사이버 방호 패러다임에서, 빠르게 피해를 복구하고 임무를 완수해내며 운용의 지속성을 유지될 수 있도록 하는 사이버 회복탄력성 보장 패러다임으로 해군의 전략적 목표를 전환할 필요가 있는 것이다.

무기체계 보안에서는 일반적으로 무기체계 수명주기 초반부터 사이버보안 관련 요소를 고려하여 사이버보안 위협을 경감시킬 수 있는 프로세스인 사이버 위험관리 프레임워크(Risk Management Framework)가 강조되는데, 해군은 수명주기가 짧은 무기를 대량으로 양산하기보다 함정을 대형화·첨단화하여 함정 숫자를 줄여가는 추세이고, 대체적으로 각 함정이 수명주기를 길게 가져가기 때문에 이미 건조가 진행 중이거나 운용되고 있는 함정·무기체계에 대한 사이버 회복탄력성을 극대화하는 전략을 택하는 것이 현실적일 수 있다.

보안 위협에 대응하는 공격·방어의 패러다임도 변화되어야 할 것이다. 전통적인 해양 안보체계에 IT보안과 OT보안의 요소를 반영한 통합보안체계의 구축이 필요하며 기존의 사이버 위협이 군의 정보망 마비, 방산정보 유출, 무기체계 무력화뿐만 아니라 물리적 환경으로까지 그 범위를 넓히면서 사이버 방어체계와 물리적 보호체계의 구축이 동시에 요구된다.

'국방사이버안보훈령'은 사이버작전을 "특정 목표 달성을 위해 사이버영역 내부에서 또는 사이버영역을 이용하여 사이버능력을 운용하는 군사작전"이라고 규정하고 있다. 사이버는 이제 작전 분야이고 사이버작전은 선택적 역량이 아니라 대한민국 해군이 지향하고 있는 첨단기술 집약형 강군, 스마트 해군(SMART Navy) 건설을 위한 필수 역량으로 취급되어야 한다.

체계적인 사이버작전 임무수행 조직 구성, 사이버작전 수행을 위한 충분한 권한 부여, 무기체계 SW통합보안관리 전문기관 설립, 방산기술 개발 단계의 보안 설계(Security by Design) 구현, 해군 내 사이버병과 또는 사이버작전 주특기 신설 등을 통해 해군의 공세적·방어적 사이버작전 역량을 강화하여 우리 해군이 스마트 해군 건설이라는 시대적

표와 기능 우선순위 측면에서 차이가 있음

소명을 완수하고 미래 해양 전장을 주도하는 해양강군(海洋强軍)으로 거듭나길 기대해본다.

※ 본고는 2020년 7월 29일 참모총장 주관으로 개최되었던 2020년도 제2차 해군정책포럼을 위한 필자의 주제발표 자료를 토대로 작성되었음

약력

임종인 교수(jilim@korea.ac.kr)는 1986년 고려대학교에서 대수학(암호학)전공으로 박사학위를 받고, 2000년부터 고려대학교 정보보호대학원, 사이버국방학과 교수로 재직 중이다. 고려대학교 정보보호대학원장, 한국정보보호학회장, 한국CISO협회장, 대통령 직속 개인정보보호위원회위원, 대통령 비서실 안보특별보좌관을 거쳐 현재는 고려대학교 정보보호대학원 명예원장, 정보보호연구원장을 역임하고 있다.

국내외 참고자료

- Ronald O'Rourke. "Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress." *CRS.* October 07, 2020.

- Mallory Shelbourne. "Navy CIO: 'Malicious Cyber Actors' Attacking Military Telework Infrastructure" *USNI News.* September 02, 2020.

- Maritime Executive. "Naval Dome: Cyberattacks on OT Systems on the Rise." *THE MARITIME EXECUTIVE,* July 26, 2020.

- News Team. "Cyber Attacks at Sea: Blinding Warships."*Cyber Defense Magazine.* July 02, 2020.

알림

- 본지에 실린 내용은 집필자 개인의 견해이며 본 연구소의 공식입장이 아닙니다.
- KIMS Periscope 는 매월 1 일, 11 일, 21 일에 카카오톡과 이메일로 발송됩니다.
- KIMS Periscope 는 안보, 외교 및 해양 분야의 현안 분석 및 전망을 제시합니다.

웹페이지보기