사이버안보연구, 2집 2호 2025 겨울, 005-055

공세적 사이버방어 전략의 법적 이해와 제도화 방안 연구*

현새롬 | 고려대학교 정보보호대학원 연구원

* 본 연구는 한국사이버안보학회의 연구용역과제(과제명: '합리적인 사이버안보 위협 대응 제도 수립방안 연구', 수행기간: 2023.08.~2023.12.) 결과물을 바탕으로 수정·보완한 것입니다.

논문접수일 2025년 10월 21일 | 논문심사일 2025년 11월 30일 | 게재확정일 2025년 12월 8일

논문 요약

오늘날 사이버안보 환경은 군사적 위협을 넘어 사회·경제 전반으로 확산되며 국가사회의 모든 영역이 국가안보 문제와 직결되고 있다. 공세적 사이버방어는 단순 차단을 넘어 위협원을 탐지·식별·무력화하고 필요시 역추적·비례 대응까지 포함하는 개념으로서 사전 침입·사전 차단·역추적·비례 대응의 네 유형으로 구분할 수 있다. 전략적으로는 방어지만 전술적으로는 공격적 성격을 띤다. 법적 분석 결과 사전 개입 필요성은 긍정되나 내국인 정보수집 등 기본권 침해 우려로 관리 절차가 요구된다. 또한 영장주의와의 충돌, 통신비밀보호법의 한계로 사전 승인, 사후 관리 절차 등을 포함하는 새로운 입법 필요성이 지적된다. 결론적으로 공세적 사이버방어 활동의 법적 근거 명문화, 사업자 협조 장려 및 관계자 면책 규정, 수집정보 관리와 다층적 감독체계 확보가 필수 과제로 제시된다.

주제어 사이버안보, 사이버안보법, 능동대응, 공세적 대응, 공세적 방어

Ⅰ. 머리말

오늘날 사이버안보 환경은 다층적 공격의 양태를 고려해야만 하는 상황이 되었다. 전통적인 안보 개념에서 나아가 경제, 사회, 일상 등 전반의 영역이 사이버안보 문제와 엮이고 있기 때문이다. 사이버 위협은 비물리적 층위, 물리적 층위, 사회적 층위, 군사적 층위 등에서 상호 연계되어 나타난다.[1] 전통적인 안보는 군사적 층위에 집중된 국가의 관심사였으나 사이버공간에서의 위협은 사회 전체의 기능을 마비시키거나 혼란을 조성하는 위협도 가능하다. 민간의 기업이나 다른 주체를 통해 진입해 공공의 영역이나 중요한 기반시설을 공격할 수도 있다. 따라서 반드시 대상이 되는 공공이나 군사시설을 굳이 직접 공격하지 않더라도 민간이나 다른 주체를 통해서도 피해를 입힐 수 있는 환경이 가능해진 것이다.[2] 이로 인해 보안 패러다임은 분야 경계를 넘어서 공급망 전체를 고려해야 하는 공급망 보안 전략으로 전환되고 있다. 특히 우리나라는 2009년 북한의 디도스 공격, 2013년 3.20 사이버테러, 2014년 한수원 원전 해킹, 2016년 국내 안보 분야 보직자 스마트폰 해킹, 2016년 군 무인정찰기를 생산하는 대한항공과 국방전산망 해킹, 2021년 한국항공우주산업 해킹, 2023년 법원 전산망 해킹, 2024년 친러 해킹그룹에 의한 국내 주요 정부기관 웹사

1) Intelligence and National Security Alliance, Cyber Intelligence: Setting the Landscape for an Emerging Discipline, INSA Cyber Intelligence White Paper, 2011, pp. 5-6.

2) 장노순, "사이버 안보위협과 사이버 방첩의 역할과 전략", 국가정보연구 제9권 제2호, 한국국가정보학회, 2016, 100면.

이트 디도스 공격, 2025년 중국이 수행한 것으로 의심되는 SKT 해킹 등의 사례들을 겪어온 실전 국가다. 아울러 최근의 사이버안보 위협은 여기서 나아가 더욱 은밀하고 일상적이며 실질적인 형태로 자리하고 있다. 기본적으로 배후를 파악하기 어려운 것은 물론 민간 주체 등 다른 기관이나 해외 서버 등을 경유하고 다크웹이나 방탄호스팅, 암호화 메신저와 암호화폐 등을 활용해 추적을 피한다. 특히 중앙행정기관 등을 대상으로 하는 사이버공격 및 위협으로 인한 사고의 경우 해킹 경유지를 민간 홈페이지 또는 국외 IP에 구축하는 경우가 많다. 본래도 침입을 당했는지 알기 어려운데 목적을 달성하고 나면 기록을 지우고 스스로를 삭제하는 형태의 기법들도 활용된다. 소프트웨어 공급망을 활용해 유지보수나 패치 등의 단계에서 악성코드를 심는 공격도 급증했다. 물리적인 공급망으로서 반도체 등 칩 단위에서의 위협도 존재한다.

이처럼 최근의 사이버안보 위협은 그 영향이 보다 직접적으로 나타나 이미 랜섬웨어나 암호화폐 탈취와 같은 재산적 피해는 물론 정부 행정망이나 공공서비스 마비, 기반시설의 파괴 등으로도 충분히 이어질 수 있는 상황이다. 이와 함께 중국의 지식재산권 탈취, 북한의 암호화폐 해킹, 방산업체 등의 첨단 기술자료나 각종 정세자료 등의 해킹 등이 상시 벌어지고 있으며 이러한 공격은 특정인을 대상으로 교묘하게 이루어지기도 하지만 앞서 본 바와 같이 공급망 공격의 형태가 늘어나며 사이버안보 대응의 영역이 확장되고 있는 상황이다. 나아가 사실상 무방비 상태의 국제규범으로 인해 유사시에 대비한 보안취약점 확보 등 무기화 경쟁도 치열하며 취약점을 수집하고 판매하는 브로커 업체들도 이미 공고하게 자리를 잡아 시장이 형성된 상태다. 사이버안보 문제가 하나의 시장으로 자리하면서 국제정치적

문제에서 나아가 경제적 문제로도 연결되고 있는 것이다. 이와 같은 위협의 변화 동향을 고려하면 사이버안보 위협 대응 방식은 공격이 들어오면 실행에 착수하는 전통적인 방어 중심의 개념에서 나아가 보다 능동적이고 선제적인 형태로 변화할 필요가 있다. 이와 함께 실제 공격이 있는 경우에는 그에 비례하는 수준의 대응을 명확히 함으로써 억지 전략을 펼칠 수 있어야 한다. 잠재 공격자가 침입을 통해 얻을 수 있는 예상 이익보다 손실이 더 클 것임을 분명히 인식시켜야 적극적 의미에서의 억지가 성공할 수 있다.[3)]

우리 정부도 선제적 방어를 강화하기 위한 논의를 진행 중이다. 2023년 11월 국가안보실은 사이버안보 상황점검 회의를 통해 범정부 선제 대응태세를 점검하면서 러시아-우크라이나 전쟁의 장기화, 이스라엘과 하마스 전쟁 발발, 북한의 가상자산 탈취 등 글로벌 사이버안보 위협 상황을 언급하며 상황이 발생할 경우 신속하게 협력할 수 있도록 국내외 공조 체계를 강화하고 위협 세력의 악의적 사이버 활동을 억지할 수 있는 역량과 선제적 방어역량 강화를 주문했다.[4)] 2024년 2월에는 국가사이버안보전략을 통해 공세적 사이버방어를 원칙으로 천명하고 같은 해 9월 보다 구체적인 내용을 담은 국가사이버안보 기본계획을 발표했다. 그러나 공세적 사이버방어 전략을 이행하기 위해서는 기본적으로 법적 근거를 마련해야 하고 실제로 어떤 행위로 구현될 수 있는지 등을 고려한 다양한 법적 쟁점을 식별

3) 박종재, 이상호, "사이버 공격에 대한 한국의 안보전략적 대응체계와 과제", 정치정보연구 제20권 제3호, 한국정치정보학회, 2017, 105면.

4) 최영훈, "국가안보실, 사이버 안보 점검…'선제적 방어 강화 노력'", 이투데이 2023.11.15. https://www.etoday.co.kr/news/view/2302691

해 이를 법제화하는 작업에 녹여낼 수 있어야 한다.

이에 본 연구는 공세적 사이버방어 전략의 이행을 위한 법적 쟁점을 식별하고 관련 개선 과제를 제안하고자 하였다. 이를 위해 먼저 공세적 사이버방어 전략의 개념화를 시도하고 이를 통해 법적 쟁점을 식별하였다. 이후 이미 공세적 사이버방어 전략을 실행 중인 선진국의 법제 동향 분석을 통해 선진 사례를 탐색하고 결론으로서 유관 제도 설계시 고려해야 하는 과제를 제안하였다.

Ⅱ. 공세적 사이버방어 전략의 법적 이해

1. 공세적 사이버방어 전략의 요구

1) 사이버안보 위협의 속성

사이버공간은 기본적으로 행위자들에 의해 구성되는 공간이라고 할 수 있다. 행위자의 의도나 행위가 사이버공간의 성격을 결정하는 중요한 변수가 되는 것이다. 기술로 직접 사이버공간을 설계, 구축하고 변화시키는 관계자가 있는 반면 그로 인해 발생하는 영향들을 목도하고 대응하는 집단도 있다. 이러한 행위자들이 사이버공간을 위험한 공간으로 보는지 안전한 공간으로 보는지의 시각에 따라 사이버공간을 대하는 전략과 행동도 달라지고 이는 결국 사이버공간 자

체의 질서와 성격을 결정하게 된다.[5] 특히 이러한 속성은 이어서 다루는 위협의 불투명성이나 공격의 우위성 등과 연계되어 구체적인 공격으로 피해가 발생하기 전에 위협을 탐지하고 위협원을 차단, 제거할 수 있어야 한다는 필요성으로 연계된다. 따라서 국가기관은 사이버공간에서의 위협 행위자를 식별하고 특성이나 기법을 이해하는 노력 등을 필수적으로 수행할 수밖에 없다.

사이버안보 위협의 또 다른 특징은 불투명성이다. 이는 기본적으로 익명성, 은밀성이나 기밀성으로 인해 행위 자체를 식별하기 어렵다는 점에 기인한다. 결과가 나타나거나 정보 등이 탈취된 사실을 인지하기 전까지는 위협의 존재 가능성을 확인할 수 없다. 실제로 사이버공간에서 공격자들은 신분을 속이는 것은 물론 디지털 추적 등 사이버억지를 회피하기 위해 다크웹이나 방탄호스팅 서버 이용을 일상화하고 다른 조직의 악성코드를 모방하거나 목표 달성 후에 모든 기록을 삭제하는 툴을 제작하는 등 최대한 스스로를 숨기기 위한 기법들을 동원한다.[6] 아울러 위협의 불투명성으로 인해 실재하는 수준의 위협을 증명하기 어려워짐에 따라 사이버안보 위협의 대응 지형도 영향을 받는다. 핵무기를 둘러싼 안보적 대응과는 달리 사이버공간의 위협은 적극적인 위협 대응이 필요한지 혹은 그것이 과장되었으므로 방어하는 수준의 대응이면 족한지에 관한 논의가 아직도 분분한 상태다. 결국 사이버공격의 안보 위협에 대한 판단은 그 효과나 공

5) 장노순, 한인택, "사이버안보의 쟁점과 연구 경향", 국제정치논총 제53집 제3호, 한국국제정치학회, 2013, 581-582면.

6) Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment", Journal of Strategic Studies 36(1), 2013, pp. 121-122.

격의 결과를 바탕으로 경험적으로 내린 것이 아니라 주로 그들의 속성과 가능성, 제한된 소수의 사례 및 가상의 시나리오로부터 추론하여 내린 것이라는 의견도 있다.[7] 이에 따라 위협을 강조하는 측에서는 위협이 실재함을 경험적으로 주장하기에 한계가 있을 수밖에 없다. 실제로 발생한 사이버공격의 결과나 사이버무기의 효과도 이견이 없을 정도로 확실하거나 심각하지 않다. 대량살상이 발생한 적도 없고 사이버공격으로 직접 인명을 상실하거나 물리적 기반이 무너진 사례도 많지 않기 때문이다. 그러나 오히려 진짜 문제는 이러한 사이버안보 위협이 극단적인 상황에 대처하기 위한 대비책 및 물리적 기반을 무너뜨릴 수 있는 자원을 탈취하는 데 더 많이 쓰이고 있다는 점이다. 중장기인 디지털 전환 경쟁을 고려할 때 사이버 위협은 실제 도시 운영이나 교통 인프라 등에 중대한 피해를 입힐 수 있는 수준으로 작용할 수 있다. 적어도 현재 상황에서는 이를 실현하지는 않지만 유사시 언제든지 활용하기 위해 전 세계 정보기관들이 보안취약점을 찾거나 구매하고 적성국 등의 기반시설에 악성코드를 심거나 적합한 사이버무기를 개발하고 있다. 나아가 사이버공격을 통해 실제 핵무기를 개발하는 자금을 조달[8]하기도 하고 첨단 전투기의 설계도를 탈취[9]하는 등 실제 안보에 영향을 미칠 수 있는 행위들을 수행하고 있

7) 장노순, 한인택, "사이버안보의 쟁점과 연구 경향", 국제정치논총 제53집 제3호, 한국국제정치학회, 2013, 583-584면.

8) 문가영, "활개치는 랜섬웨어, 전시엔 핵무기 될 것", 매일경제 2023.09.12. https://www.mk.co.kr/news/economy/10828014

9) 연합뉴스, "美 F-35 전투기 설계정보, 중국 스파이가 빼돌려", 2015.01.19. https://www.yna.co.kr/view/MYH20150119018500038

다. 이러한 점에서 2020년 솔라윈즈 IT 관리 솔루션 오리온 업데이트를 활용한 공급망 공격, 2022년 콜로니얼 파이프라인 랜섬웨어 공격 등 실제로 드러난 사건들도 중요하지만 잠재적인 취약점과 사이버무기 문제가 더 심각하다고 볼 수 있다.

마지막으로 사이버안보 환경에서 공격은 근본적으로 방어에 비해 우위에 있다. 일례로 공격자는 수많은 프로그램에서 하나 이상의 취약점을 찾아내면 그 목적을 달성하지만 방어자 측은 모든 취약점을 망라하여 검증하고 업데이트를 계속해야 하기 때문이다. 그 비용의 차이는 너무 크기 때문에 여전히 공격자 측에 선제공격은 매력적인 카드일 수밖에 없다.[10] 아울러 디지털 전환이 확대된다는 점도 공격을 더욱 유리하게 만든다. 방어하는 입장에서는 공격 루트를 예측할 수 없고 공격 표면도 늘어나기 때문에 근본적으로 비대칭적 균형에 놓일 수밖에 없기 때문이다. 특히 기반시설 등 산업제어시스템의 영역, 스마트시티와 같은 경우에는 사소한 결함이 국가안보와 국민 안전에 영향을 미치는 치명적 결과로 이어질 수도 있다. 인명피해까지 이어지진 않더라도 최소한 국가의 전략 체계를 훼손할 가능성도 높다.[11] 북한 또한 저비용 고효율이라는 이점을 최대한 활용하기 위해 사이버 위협 역량을 계속 키우고 각종 해킹이나 사이버 공작 등을 수행하고 있다.[12]

10) 윤정현, "인공지능과 블록체인의 도입이 사이버 안보의 공·수 비대칭 구도에 갖는 의미", 국제정치논총 제59집 제4호, 한국국제정치학회, 2019, 56면.

11) 윤정현, "인공지능과 블록체인의 도입이 사이버 안보의 공·수 비대칭 구도에 갖는 의미", 국제정치논총 제59집 제4호, 한국국제정치학회, 2019, 54면.

12) 유동열, "북한의 사이버 위협 실태와 대응", 전략연구 제28권 제3호, 한국전략문제연구소,

2) 사이버안보 패러다임의 변화

가장 돋보이는 변화는 공공과 민간의 경계가 더욱 빠르게 붕괴되고 있다는 점이다. 디지털 전환으로 두 영역의 결합이 강해지면서 나타나는 현상이다. 대표적인 예가 클라우드 전환이다. 각국 정부의 클라우드 전환 전략으로 사실상 민간의 클라우드 서버를 활용하는 사례들이 늘어나고 있기 때문이다. 국가정보원 또한 공공영역에 확대중인 민간 클라우드의 보안취약점 집중 공격 우려를 제기한 바 있다.[13] 이러한 환경에서는 민간의 협조가 필수적이다. 국가기관으로서는 사이버위협의 징후를 발견했다면 이를 추적, 조사하기 위해 클라우드 서비스 제공자 등의 협조를 얻어 서버 내 경로나 특징 등 상세정보를 제공받아야 한다. 그러나 여기에는 여러 문제들이 엮일 수밖에 없다. 서버의 정보를 제공해야 하는 업체는 이용자들의 비판이나 소송 문제에 대응하여야 한다. 정보를 제공받기 위해 기관 입장에서는 영장을 받아 협조를 요청하는 절차가 필요하기도 하다. 해킹 영장을 받을 수 있는 때에는 직접 서버나 대상자 기기에 접속해 필요한 정보를 얻을 수도 있다. 이 경우에도 국가의 감시 우려 등이 발생함은 물론이다. 이와 같은 문제를 반영한 민관협력 제도의 설계가 요구되는 것이다. 한편, 이러한 경계 붕괴의 핵심 요인은 공급망 보안 위협이라고 할 수 있다. 공급망 공격이 국가적 주요 사이버안보 문제로 대두되며 각국은 사이버보안 활동의 일환으로 ICT 공급망 위험관리 정책을 시행하며 안전한 공급망 환경을 구축하기 위한 제도를 마련하

2021, 11면.

13) 국가정보원, “2022년 사이버안보 위협 주요 특징 및 내년 전망”, 2022.

였다. 이에 인증된 제품에 대하여 추가적인 보안성 검증과 함께 공급망 공격에 대한 탐지 및 선제적 대응, 피해 발생 후 발생 위치 파악, 피해 범위 산정, 신속한 후 속 조치를 위한 방책으로 공급망 가시화 및 무결성 보증에 대한 필요성이 논의되고 있다.[14)]

3) 사이버 억지효과의 요구

억지란 상대방으로 하여금 자신이 기대하는 이익보다 비용이 초과할 것이라고 믿게 함으로써 어떤 행동의 수행을 단념하게 하는 것으로 정의된다. 이러한 억지의 유형은 보복이 두려워 공격을 하지 못하도록 하는 보복에 의한 억지, 공격해도 효과가 없어 의지를 꺾도록 하는 거부에 의한 억지, 공격자 자신에게도 영향을 미칠 수 있다는 점을 활용하는 연루에 의한 억지, 국제사회 차원에서의 각종 규제나 제재를 가하는 규범에 의한 억지로 구분된다.[15)] 이러한 억지전략이 실질적으로 구현되려면 먼저 억지의 대상을 명확히 식별할 수 있어야 한다는 문제가 있다. 그리고 이를 통해 어떤 형태로든 경고 메시지를 명확히 전달하여 공격을 단행하지 못하도록 하는 효과를 얻을 수 있어야 한다.

그러나 사실상 공격 행위자나 최종 의사결정자 등을 특정하기 어려운 문제들로 인해 실질적인 억지 효과를 얻기는 어렵다.[16)] 이를 해

14) 손효현, 김동희, 김소정, “사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구: SBOM 정책 추진 사례를 중심으로”, 디지털융복합연구 제20권 제2호, 2022, 10면.

15) 김상배, “사이버 억지의 새로운 개념화: 한미 사이버안보 동맹론의 성찰적 맥락에서”, 국제정치논총 제63집 제2호, 한국국제정치학회, 2023, 66면.

16) 윤정현, “인공지능과 블록체인의 도입이 사이버 안보의 공·수 비대칭 구도에 갖는 의미”, 국제

결하려면 결국 선제적이고 상시적으로 대상을 면밀히 살필 수 있는 체계가 요구될 수밖에 없다. 이와 더불어 실질적인 공격의 피해도 점차 커지고 심각해짐에 따라 결과가 발생하기 전에 실질적으로 억제해야 하는 필요성도 증가하였다. 이와 같은 상황이 도래하자 공세적 방어(active defense)라는 개념이 등장하였다. 공세적 방어는 '위협에 대하여 단순히 자신의 네트워크를 철저히 방어하는 것을 넘어 특정 사이버 작전을 수행한 주체를 밝혀내거나 그 주체의 시스템을 불능화하는 대응조치로 정의된다.[17)]

이러한 공세적 방어의 기준은 첫째, 방어는 자신의 네트워크 안에서만 이루어지는가, 아니면 중립적인 제3의 서버 또는 사이버 작전 수행자의 시스템 등 자신의 네트워크 경계 밖에서 이루어지는가? 둘째, 방어 행위 시 상대방 시스템상에 식별 가능한 효과가 발생하는가, 아니면 시스템상의 프로그램이나 데이터에 어떠한 실질적 변화도 일으키지 않은 채 단순히 감시만 수행하는가? 등으로 구분해볼 수 있다.[18)] 예를 들어 역해킹은 악의적 활동을 중단시키거나 그 효과를 억제하기 위하여, 또는 귀속 문제를 해결하는데 사용될 수 있는 기술적 증거를 수집하기 위하여 이루어진다.[19)] 따라서 이 또한 악의적인 사

정치논총 제59집 제4호, 한국국제정치학회, 2019, 59면.

17) Anthony D. Glosson, "Active Defense: An Overview of the Debate and a Way Forward", Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, 2015, p. 4.

18) Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures", Stanford Journal of International Law, Vol. 50, Issue 1, 2014, p. 105.

19) Michael N. Schmitt et al.(eds.), TALLINN Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, p. 565.

이버공격의 근원지를 찾고 차단하기 위해 적극적인 행동을 취하는 것을 주목적으로 하므로 공세적 방어의 일종이 될 수 있는 것이다. 특히 최근의 억지전략을 고려하자면 오늘날이 공세적 방어 활동은 단순히 사전 예방적 차원에서만 국한되는 것이 아니라 사후적 결과에 대해서도 유연하게 대응하는 등 전후방 전반을 고려해 수행될 필요가 있다. 결국 사전 위협 탐지를 위한 감시 활동에서부터 사후 결과에 대한 역추적 및 비례하는 수준의 보복행위를 포함하는 활동들이 그 범위라고 할 수 있을 것이다.

2. 공세적 사이버방어 전략의 개념화

1) 공세적 사이버방어 활동의 판단 기준

공세적 사이버방어의 개념들을 두루 살펴보면 공통적으로 근원지, 행위자의 식별, 위협원의 불능화, 무력화 및 완화와 같은 용어들을 뽑아볼 수 있다. 이러한 점에서 살펴보면 능동적 사이버안보 활동의 기준은 크게 ① 행위의 범위 및 ② 행위의 목적으로 구분해 볼 수 있다.

먼저, 공세적 사이버방어 활동을 판단하기 위한 대표적 기준 중 하나는 행위의 범위로서 이는 영역 외에서 수행되는 것인지의 여부라고 할 수 있다. 원 행위자를 식별하기 위해 근원지를 찾아 역추적하는 것이 본질 중 하나이기 때문에 네트워크 내부에서 나아가 외부에서의 활동이 요구된다. 이러한 과정에서는 외부 네트워크의 흔적을 탐색하고 추적하는 과정들을 수행해야 하므로 특정 국가나 기업의 협조를 받아야 할 상황이 다수일 수밖에 없다. 또한 대상이나 위협원을 무력화 또는 완화하는 등 적극적 조치가 이루어져야 하기 때문에 고려하지 못한 내국인의 정보를 수집할 가능성도 있다.

또 다른 기준은 행위의 목적이다. 목적을 구분하는 이유는 그러한 활동이 자칫 공격 목적으로 악용되어서는 안 되고 외부에서도 그렇게 보이지 않아야 하기 때문이다. 본래 공세적 방어라는 관점에서는 특정 위협이 있는 경우에 결과가 발생하기에 앞서 대응하는 행위에 한정될 것이다. 그러나 사이버안보 활동의 관점에서는 보다 적극적으로 적대적인 해커단체나 조직, 개인 등을 추적하고 사이버 역량으로 와해하거나 수사로 넘기는 등의 행위들을 포함한다고 보는 것이 타당하다. 따라서 공세적 사이버방어 활동은 위협원을 선제적으로 탐지하고 차단하며 사후적으로도 원점을 식별해 타격하는 행위들을 모두 포함한다고 볼 수 있다.

이러한 점에서 행위의 시점은 큰 기준이 되지 못한다. 위협의 결과가 발생하기 전이라도 적극적으로 적성국이나 해커단체의 행위를 감시할 수 있어야 하고 위협행위에 착수하기 전에 이를 차단하는 행위, 위협이 이루어지고 결과가 발생하였다면 이를 추적해 대응하는 행위들이 모두 포함되기 때문이다.

행위의 수단도 기준이 될 수 없다. 본래 관념상 수동적 정보수집 활동에는 감청과 같은 감시활동, 적극적 정보수집 활동에는 해킹 등의 활동들이 포함되는데 공세적 사이버방어 활동은 이를 모두 포괄하는 것으로 달리 봐야할 필요가 있다. 즉, 위협에 앞서 실제 위협원으로 발전할 수 있는지 여부를 식별, 탐지해야 하므로 대상 서버나 기기에 침투해 감시하는 행위가 있어야 하고 필요한 경우 적극적인 개입으로 위협행위를 차단하거나 위협원을 제거해야 하기 때문이다. 이런 과정에서는 사회공학적 기법을 활용할 수도 있고 역추적 등 중간 단계에서는 특정 기업이나 기관의 협조를 받아야 할 필요도 있으며 취약점을 찾거나 구매해 적합한 해킹 도구를 만들고 악성코드를 제작

해야 할 필요도 있을 것이다. 트래픽 경로를 조작해야 하고 랜섬웨어나 와이퍼 소프트웨어 등을 활용해야 할 수도 있다.

이러한 점을 종합적으로 고려할 때 공세적 사이버방어 활동의 특성을 살펴보면 다음과 같다. 먼저 공세적 사이버방어 활동은 전략적 수준에서는 방어적인 개념이지만 실제 전술적, 작전적 차원에서는 공격적일 수 있다. 이러한 점에서 공세적 사이버방어 활동에 활용되는 수단이나 기법은 사이버공격에 사용되는 그것과 동일하거나 유사할 수 있다.[20] 둘째, 보복행위나 제재, 대응 등이 활용될 수는 있겠지만 이 또한 근본적 목적이 아닌 수단에 불과하고 실질적인 속성은 악의적 사이버 활동의 영향을 종식시키거나 완화하는 것을 목표로 한다.[21] 개념상 주체는 국가기관뿐만 아니라 협력하는 다른 국가의 기관 등도 포함된다. 집단적 사이버안보 활동도 가능하기 때문이다. 종합하여 볼 때 공세적 사이버방어 활동이란 "국가 또는 국가들이 기술적 수단과 역량을 활용해 특정 사이버 위협을 탐지, 식별, 예방하고 위협이 발생한 때에는 근원지를 밝혀 행위를 귀속시키고 그 영향을 완화하거나 무력화시키는 행위"라고 정의할 수 있다.

2) 공세적 사이버방어 활동의 유형

공세적 사이버방어 활동의 개념에서 살펴보면 활동의 유형은 크게 ① 사전 탐지 관점에서 적의 기기에 침투해 위협정보를 수집, 감시하

20) Sven Herpig, "Active Cyber Defense Operations", Stiftung Neue Verantwortung, 2021, p. 11.

21) Sven Herpig, "Active Cyber Defense Operations", Stiftung Neue Verantwortung, 2021, p. 12.

는 행위, ② 공격할 것으로 보이는 경우 사전 차단하는 행위, ③ 공격을 받은 경우 수법과 경로를 조사해 역추적하는 행위, ④ 추적 후 비례적 대응을 하는 행위로 구분해 볼 수 있다. 이러한 행위의 예시로는 사전에 위협원으로 의심되는 시스템 등을 감시하고 이상행위 확인 시 차단하는 행위, 악성 트래픽을 차단하거나 경로를 변경하는 행위, 특정 위협행위자가 자주 활용하는 서비스나 사이트 등을 허위로 구축해 우회하여 정보를 획득하는 허니팟, 봇넷과 같은 악성 사이버 캠페인에 사용되는 감염 시스템이 해커의 명령 및 제어 서버를 활용하는 경우 이를 식별해 싱크홀 서버로 응답 주소를 변경하는 행위, 위협행위자의 명령 및 제어 인프라를 장악해 멀웨어를 제거, 무력화하고 패치를 배포하는 행위, 시스템에 침입하여 탈취한 정보나 자료 등을 삭제하거나 시스템을 무력화하는 행위 등이 해당될 수 있다. 실제로 2012년 이란 해커들은 2010년 스턱스넷 공격에 대한 보복으로 사우디아라비아의 석유회사 아람코를 공격해 아람코 컴퓨터 데이터의 대부분을 삭제하고 불타는 성조기 이미지로 대체하는 결과를 야기했다.[22] 또한 미국은 2014년 소니 해킹 사건에 대한 보복으로 북한의 인터넷을 마비시켰으며[23] 2020년에는 사이버사령부 차원에서 러시아가 주도하는 것으로 알려진 세계 최대 봇넷 Trickbot을 무력화하여

22) Nicole Perloth, “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back”, 2012.10.23. The New York Times, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

23) Eric Tucker, “North Korea Internet outage in wake of Sony attack over”, 2014.12.23. AP, https://apnews.com/united-states-government-general-news-34ad411e0c9945a6a1d608ef54e988cf

대선 전 공세적 대응을 수행했다.[24)]

3. 공세적 사이버방어 전략의 법적 분석

1) 예방적·적극적 조치의 법적 속성

공세적 사이버방어 전략의 핵심은 구체적인 위험이 발생하기 전에 공권력의 개입이 이루어져야 한다는 데 있다. 이러한 논리는 새로운 위험 및 리스크 대응을 위해 요청되었던 경찰법의 변화로부터 도출할 수 있다. 위험이 오늘날 사회의 한 구성요소라는 울리히 벡의 위험사회론에 입각하여 늘 발생할 수밖에 없는 위험에 대한 대응 및 방지가 요구되고 있기 때문이다. 이러한 관점에서 독일에서는 위험을 사전에 방지하지 않으면 효과적인 대응이 어렵다고 판단되는 때에는 경찰기관이 위험의 전 단계에서 개입할 수 있어야 한다는 정책적 주장으로서 사전배려의 원칙이 발전하기 시작했다.[25)] 사이버안보 위협의 경우에도 마찬가지라고 판단된다. 충분한 억제력을 확보함으로써 필요한 경우 언제든 원점을 식별해 무력화할 수 있다는 역량을 보여주는 것도 중요한 전략적 요소다.[26)] 그러나 더 중요한 것은 국가의 기반시설과 국민의 일상에 피해가 발생하기 전에 이를 보호하기 위한

24) Shannon Vavra, “Cyber Command, Microsoft take action against TrickBot botnet before Election Day”, 2020.10.12. Cyberscoop, https://cyberscoop.com/trickbot-takedown-cyber-command-microsoft/

25) 이기춘, “독일 경찰질서행정법상 위험방지론과 리스크대비론의 현대적 변화에 관한 연구”, 법학논고 제62집, 경북대학교 법학연구원, 2018, 48-49면.

26) 이상호, “사이버 공격에 대한 적극적 억제 능력 확보 필요성 연구”, 국가정보연구 제18권 제1호, 한국국가정보학회, 2025, 83면.

실질적인 조치로서 공세적 사이버방어 전략을 이해해야 한다는 점이다. 한편, 이러한 접근은 적극적인 유형의 공세적 사이버방어 활동에 적용되는 것이고 그에 이르지 않는 수준으로서 단순히 사전 위협 탐지를 위해 위협정보를 수집, 감시하는 등의 행위를 수행한다면 이는 구체적인 위험 예방 행위라기보다는 정보활동의 성격에 가깝다고 볼 수 있다. 따라서 이러한 정보활동은 위험에 이르지 않는 리스크 단계에서 충분히 시작될 수 있는 것이고 국가 본연의 역할로 이해되는 것이므로 경찰법상 사전배려의 원칙을 요구하지 않더라도 그 자체만으로 정당성이 인정된다고 할 수 있다. 사이버테러나 국가 단위의 사이버공격을 막기 위한 사전 위협탐지 활동이라면 물리적 공간에서도 일반적인 테러나 국가안보 위협을 사전에 탐지하기 위한 정보활동으로 볼 수 있기 때문이다. 다만, 문제가 될 수 있는 지점은 이러한 사전 위협탐지를 위해 대상의 기기에 침투해야 한다는 점에서 자칫 제3자의 정보를 탐지할 수 있게 되는 등 시민의 자유를 침해하게 되는 경우이다. 실제로 이와 같은 활동을 수행하는 것이 불가피하다면 오늘날 스마트폰이나 데이터 처리의 속성을 고려할 때 타인의 정보를 획득할 가능성이 높으므로 데이터 관리 의무 등을 부여하고 구체적인 관리 지침 마련, 사후 관리감독 등이 병행될 수 있어야 한다.

2) 영장주의의 적용 필요성

위와 같은 법적 속성에도 불구하고 현재 이를 정당화할 수 있는 법적 절차가 부재하다는 점에서 형사법적 문제를 검토할 필요가 있다. 수사기관의 온라인수색과 같은 행위가 결국 사이버안보 활동에서의 공세적 사이버방어 관념이 될 수 있다. 이 경우에는 영장주의 관점에서의 탐색이 요구되는데 공세적 사이버방어 행위는 상당 부분에서

강제처분의 성격을 띨 수 있기 때문이다. 우리 헌법 제12조제1항은 "모든 국민은 신체의 자유를 가진다. 누구든지 법률에 의하지 아니하고는 체포·구속·압수·수색 또는 심문을 받지 아니하며, 법률과 적법한 절차에 의하지 아니하고는 처벌·보안처분 또는 강제노역을 받지 아니한다."고 규정하여 강제수사법정주의를 명시하고 있다. 또한 헌법 제12조제3항은 "체포·구속·압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다고 규정한다. 다만, 현행범인인 경우와 장기 3년 이상의 형에 해당하는 죄를 범하고 도피 또는 증거인멸의 염려가 있을 때에는 사후에 영장을 청구할 수 있다."고 규정하고 있고, 헌법 제16조는 "모든 국민은 주거의 자유를 침해받지 아니한다. 주거에 대한 압수나 수색을 할 때에는 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다."고 규정하여 강제수사에 대한 영장주의를 명시하고 있다.

관련하여 사이버안보 활동의 경우 수사로 볼 수는 없으나 강제집행의 관점에서는 영장주의가 적용될 필요성도 있다. 예를 들어 통신비밀보호법에 따른 통신제한조치가 대표적이다. 동법 제7조에 따르면 국가안보 목적으로 정보수집이 필요한 경우 통신의 일방 또는 쌍방이 내국인인 경우 고등법원 수석판사의 허가를, 외국인 등에 관한 경우에는 대통령의 승인을 받도록 하고 있다. 이와 같은 점에서 법원의 영장을 받든 제3기관의 검토 및 승인을 받든 어떤 형태로든 영장주의의 적용은 필요하다고 생각된다. 한편, 통신비밀보호법을 적용해 공세적 사이버방어 활동을 수행할 수 있는지 여부도 문제될 수 있는데 현재 동법에 따른 통신제한조치는 우편물의 검열 또는 전기통신의 감청을 뜻하고 감청은 전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청

취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다. 이와 관련하여 대법원은 전기통신이 이루어지고 있는 상황에서 실시간으로 그 전기통신의 내용을 지득·채록하는 경우와 통신의 송·수신을 직접적으로 방해하는 경우를 의미하는 것이지 이미 수신이 완료된 전기통신에 관하여 남아 있는 기록이나 내용을 열어보는 등의 행위는 포함하지 않는다고 판시한 바 있다.[27] 아울러 감청설비 또한 대화 또는 전기통신의 감청에 사용될 수 있는 전자장치·기계장치 기타 설비를 말한다고 하여 소프트웨어를 활용한 해킹 등이 허용될 수 있는지 명확하지 않다.

결국 현행법상 해킹은 허용되지 않는 상황이므로 새로운 입법이 요구되는 바, 이런 상황에서의 공세적 사이버방어 활동은 앞서 본 바와 같이 조직법적 권한만으로 수권이 이루어지는 것인지도 모호하여 명확한 법적 통제 아래 둘 필요가 있다고 생각된다.

3) 정당방위의 인정 여부

아울러 원점을 식별해 무력화하는 등의 조치가 정당행위나 정당방위에 해당하는지 살펴봐야 한다. 형법 제21조 제1항에서는 "현재의 부당한 침해로부터 자기 또는 타인의 법익(法益)을 방위하기 위하여 한 행위는 상당한 이유가 있는 경우에는 벌하지 아니한다"라고 규정하여 자기보호와 법질서수호의 관점에서 위법성 조각사유인 정당방위에 대해 규정하고 있다. 정당방위는 ① 정당방위상황(자기 또는 타인의 법익에 대한 현재의 부당한 침해)이 존재해야하고 ② 방위의사에 기한

27) 대법원 2016. 10. 13. 선고 2016도8137 판결

방위행위가 있어야 하며 ③ 방위행위에 상당한 이유가 인정되어야 할 것을 요구한다.

먼저, 자기 또는 타인의 법익에는 모든 개인적 법익이 포함된다. 따라서 사이버공격이 개인의 생명·신체·재산 등에 침해를 가져온 경우 이에 해당됨은 이론이 없을 것이다. 관련하여 사회적·국가적 법익도 포함할 수 있는지 문제되는데 이 경우에는 부정설이 제기되기도 한다.[28] 그러나 사회적·국가적 법익이 명백하고도 중대한 위험에 빠진 상황에서 국가기관에 의한 보호조치가 미치지 않을 경우 예외적으로 개인의 정당방위가 허용될 수 있다는 제한적 긍정설이 타당하다고 볼 여지도 있다.[29] 국가 소유의 건물 또는 물건 등에 대한 손괴 등과 같이 국가의 개인적 법익이 문제되는 경우에는 정당방위가 가능하다. 침해의 현재성과 관련하여 이미 사이버공격을 통해 피해가 발생한 이후 일정 시간이 지나 원점을 식별, 타격하게 된다면 현재성이 인정되기가 어려울 것으로도 보인다. 그러나 여전히 다른 루트 등으로 공격이 지속되거나 데이터가 유출되고 있는 등 계속범으로 볼 수 있는 경우에는 범죄가 기수에 이른 후 범죄가 종료된 시점까지 현재성의 종기로 포함될 수 있기에 현재성은 인정될 수 있다. 예를 들어 해커의 침입 사실을 확인한 상황에서 해커를 추적해 기기를 공격하여 위협을 원천 차단한다면 침입이 실시간으로 이어지고 있거나 공격 즈음하여 해커도 공격 사실을 식별하고 공격을 철회하는 등의 결과에 이를 수 있는데 이런 관점에서는 현재성의 인정 여지가 있을 것이

28) 김성돈, 「형법총론(제5판)」, SKKUP, 2018, 274면.

29) 이재상, 장영민, 강동민, 「형법총론(제10판)」 박영사, 2019, 247면.

다. 방위의사와 관련하여 적극적 반격을 넘어서 보복적 행위를 하는 것은 허용되지 않는다. 대법원도 싸움이 벌어진 경우 일방의 행위만을 위법한 침해행위라고 볼 수 없고 방위의사가 아닌 공격 의사를 가지고 상호 간의 침해를 유발한 때에는 정당방위를 인정하지 않고 있다.[30] 마지막으로 상당성이 인정되기 위해서는 필요한 범위 내의 방어여야 하나(필요성), 반드시 다른 피난 방법이 없었을 것이라는 보충성의 원리을 요하지 않고, 침해된 법익이 방위된 법익을 가치적으로 초과하지 않을 것(균형성의 원리)을 요하지는 않는다. 대법원은 정당방위의 성립 요건으로서 방어 행위에는 순수한 수비적 방어뿐 아니라 적극적 반격을 포함하는 반격방어의 형태도 포함된다고 본다. 다만 정당방위로 인정되기 위해서는 자기 또는 타인의 법익침해를 방어하기 위한 행위로서 상당한 이유가 있어야 한다. 이때 방위행위가 상당한 것인지는 침해행위에 의해 침해되는 법익의 종류와 정도, 침해의 방법, 침해행위의 완급, 방위행위에 의해 침해될 법익의 종류와 정도 등 일체의 구체적 사정들을 참작하여 판단하여야 한다고 판시하고 있다.[31]

한편, 공세적 사이버방어 활동을 수행하는 자에 대하여 형사법적 문제를 검토하는 단계까지 나아가는 것이 정당하지 않을 수 있다. 국가사이버안보 목적으로 수행한 활동이 명확한 법적 근거가 없는 상황, 또는 근거가 있더라도 해석이 모호하여 불법행위가 될 가능성이 높다면 실질적이고 적극적인 방어 활동을 수행하기 어려울 것이기 때문이다.

30) 대법원 1996. 9. 6. 95도2954 판결, 대법원 2000. 3. 28. 2000도228 등

31) 대법원 2023. 4. 27. 선고 2020도6874 판결 등

따라서 행위자에 대한 면책 규정도 함께 설계할 수 있어야 한다.

Ⅲ. 주요국의 공세적 사이버방어 관련 법제 분석

1. 미국

미국은 2023년 3월 발표한 국가 사이버안보 전략(2023 National Cybersecurity Strategy)을 통해 위협 행위자에 대한 무력화를 중점 전략으로 제시하였다. 이를 통해 국익을 위협하는 행위를 수행하는 위협 행위자를 무력화하고 이들을 해체하기 위한 모든 국력 수단을 사용할 것이라고 강조하였다.[32] 미국은 연방기관과 비연방기관이 협력하여 관련 법 집행을 통한 제재, 개인에 대한 금융적, 정보적 제재, 국가에 대한 외교적, 금융적 제재, 사이버공간을 이용한 대응 작전 수행 등을 통해 사이버공격에 대응해왔다.[33] 동 전략을 통해 미국은 가용한 모든 도구를 전략적으로 활용하여 악의적인 행위자에 대한 제재를 지속적으로 이어 나갈 계획임을 확인할 수 있다.

관련하여 직접적인 유관 법률을 제정하여 권한을 부여하고 있는

32) The White House, “National Cybersecurity Strategy”, 2023, p. 14.

33) 김소정, “2023 미국 사이버안보 전략 주요내용과 한국에의 시사점”, INSS 이슈브리프 423호, 국가안보전략연구원, 2023, 4면.

것은 아니다. 다만, 미국의 경우 기존 정보기관, 수사기관, 군기관에 권한을 부여하고 있는 행정명령과 법률에 근거하여 작전을 수행하는 것으로 보인다. 1978년 제정된 해외정보감시법(Foreign Intelligence Surveillance Act, FISA)은 미국과 관련된 외국 세력 또는 대리인에 의한 공격 또는 적대 행위, 국제적인 테러 행위, 비밀 정보 활동 등과 같은 공격으로부터 미국을 보호하는 데 필요한 정보와 미국의 국방, 안보, 외교 업무를 목적으로 필요한 외국 세력 또는 외국 영토에 관한 정보를 감시하기 위한 법률이다. 이러한 정보에는 포괄적으로 사이버안보 관련 위협정보 등도 포함될 수 있음은 물론이다. 동법 제1802조(a)(1)는 법무부장관의 서면 승인을 통해 별도의 법원 영장 없이 최대 1년간 해외정보를 수집하기 위한 전자감시의 승인 권한을 대통령에게 부여한다. 한편, 해외정보의 수집 과정에서 미국인의 정보를 수집하지 않거나 최소화할 수 있도록 필요한 절차를 취하고 그럼에도 불구하고 정보활동에 미국인이 연관되었다는 사실을 알게 된 경우, 정보수집이 시작된 후 72시간 이내에 법원의 영장을 획득하여야 한다.

아울러 정보활동에 관한 행정명령(Executive Order 12333 United States Intelligence Activities) 또한 미국 정보기관들의 해킹과 해외정보 수집을 위한 중요한 근거다. 일례로 NSA가 수행하는 대부분의 해외정보 수집은 주로 행정명령 제12333호를 통해 규율되며 해킹도 이를 근거로 수행되고 있다.[34] 동 명령은 특히 1.12조(b)를 통해 국가안보국(NSA)에게 국가안보 목적을 위한 각종 통신, 신호정보의 수집·처리·

34) Amos Toh, Faiza Patel and Elizabeth Goitein, "Overseas Surveillance in an Interconnected World", Brennan Center for Justice, 2016, p. 1.

전파 등을 수행할 수 있는 권한 등을 부여하고 있다.

2. 영국

영국은 2016년 국가사이버안보 전략(National Cyber Security Strategy 2016 to 2021)을 통해 최초로 국가 차원의 능동적이며 공세적인 사이버 안보 대응 방안을 제시하였다. 특히 능동적 사이버방어 활동은 실제 방어에 치중된 조치로서 사이버보안 수준을 향상하고 복원력을 최대로 끌어올리는 데 목적을 둔다.[35] 반면, 공세적 사이버안보 대응 활동은 실제 적의 시스템 또는 네트워크를 손상·중단 또는 파괴할 수 있는 사이버안보 능력을 갖추기 위한 기반 마련을 목표로 하고 있다.[36]

영국 또한 미국과 마찬가지로 별도의 사이버안보 활동을 수행할 수 있는 법률을 두고 있지 않고 기존 정보활동 관련 법률들을 활용하고 있다. 특히 영국의 수사권법(Investigatory Powers Act 2016, IPA)은 국가안보와 중범죄의 예방 및 탐지 등을 목적으로 하는 수사기관과 정보기관의 정보활동에 관한 사안들을 규정하는 법률이다. 특히 장비간섭(Equipment Interference)이라고 정의된 해킹 개념과 더불어 이를 활용한 정보수집의 절차로 ① 특정 장치에 대한 대상 특정 장비간섭영장(Targeted Equipmet Interference Warrant, TEIW), ② 특정되지 않은(해외 관련) 다수의 개인 또는 장치를 대상으로 하는 대량장비간섭영장(Bulk Equipment Interference Warrant, BEIW)등을 통해 정보수집의 근

35) UK HM Government, “NATIONAL CYBER SECURITY STRATEGY 2016-2021”, p. 10.

36) UK HM Government, “NATIONAL CYBER SECURITY STRATEGY 2016-2021”, p. 51.

거를 마련하고 있다.[37] 실제로 법 제102조에 따른 대상 특정 장비간섭영장은 특정 장치를 집행 대상으로 하며 국가안보, 중대범죄의 예방 및 적발, 경제적 안녕 등을 목적으로 통신(Communications), 장비데이터(Equipment Data) 그리고 기타 정보(Any other information)를 수집할 수 있도록 한다. 대량 장비간섭영장은 특정성을 요구하지 않고 해외의 세력을 대상으로 하는 국외용 영장으로서 해외 정보기관의 요구사항으로 도입된 규정이다.[38]

한편, 수사권법 제99조에 따르면 그러한 영장 집행에 필요한 부수처분으로서 통신, 장비데이터, 기타 정보를 취득하기 위한 행위를 허용하는데 이에 관한 구체적인 장비간섭 실무지침(Equipment Interference - Code of Practice)에 따르면 감시소프트웨어의 설치도 허용된다. 여기서 감시소프트웨어란 영장을 발부받아 집행할 때 소프트웨어의 보안취약점을 활용하여 키로거(Keylogger) 프로그램과 같은 각종 감시프로그램을 원격(Remotely)으로 설치하거나 컴퓨터나 모바일 장비에 당사자 몰래 직접 접속하여 감시프로그램을 설치하거나 관련 자료를 내려받는 이른바 물리적인(Physically) 방법을 모두 포함한다.[39]

3. 일본

37) 이해원, "영국의 사이버 안보 법제 변천 과정 및 시사점", 「법학연구」 제26권 제4호, 경상대학교 법학연구소, 2018, 273-277면.

38) Boukals, C, "Overcoming Liberal Democracy: 'Threat Governmentality' and the Empowerment of Intelligence in the UK Investigatory Powers Act". Studies in Law, Politics, and Society, Emerald Publishing Limited, 2020, p. 9.

39) UK Home Office, "Equipment Interference - Code of Practice, Home Office", 2018, p. 10.

일본은 2025년 5월 중요 전자계산기 부정행위로 인한 피해방지 법안(사이버 대응능력 강화법안)[40]을 통과시켰다. 동법은 기본적으로 사이버공격 대응 및 실태파악을 위한 민관협력, 통신정보의 취득 등에 관한 사항을 규정하고 있는데 이와 더불어 함께 추진된 중요 컴퓨터에 대한 부정한 행위로 인한 피해 방지에 관한 법률의 시행에 수반되는 관계 법률의 정비 등에 관한 법률(정비법안)[41]에 따르면 경찰 및 자위대의 사이버공격 무해화 조치가 도입되었다. 이에 따라 경찰관직무집행법이 개정되어 사이버위협 대응을 위한 경찰의 무해화 조치 권한과 절차가 규정되었고 자위대법 또한 개정되어 내각총리대신의 명령에 따라 필요한 조치를 취할 수 있도록 하였다.

구체적으로 경찰관직무집행법 제6조의2에 따르면 경찰청은 사이버위해방지조치집행관을 임명하고 그로 하여금 사전에 사이버통신정보감리위원회의 승인을 얻어 위협원이라고 생각되는 특정 가해관계 전자계산기를 대상으로 가해관계 전자적 기록의 소거 등 기타 위험 예방을 위해 통상 필요하다고 인정되는 조치를 취할 수 있도록 하였다. 또한 자위대법 제81조의3을 통해 내각총리대신이 사전에 방위대신 및 국가공안위원회와 협의하여 자위대로 하여금 이른바 통신방호조치를 취할 수 있도록 하고 있다.

Ⅳ. 공세적 사이버방어 제도의 설계 과제

40) 重要電子計算機に対する不正な行為による被害の防止に関する法律案

41) 重要電子計算機に対する不正な行為による被害の防止に関する法律」の施行に伴う関係法律の整備等に関する法律

1. 공세적 사이버방어 행위별 고려사항

1) 사전 침입 및 탐지 행위

전통적인 법질서에 따르면 공권력의 개입은 결과가 있는 때에 법률에 근거하여 허용 가능하다. 그러나 사이버안보 위협의 특성을 고려하면 결과가 발생한 후에는 원상복구가 어렵고 필요한 조치를 취하기 어렵다는 한계가 존재한다. 이러한 점에서 위협에 대응하려면 사전에 주요 위협 국가 또는 단체 등을 탐지하고 위협을 식별할 수 있어야 한다. 이와 같은 행위는 사이버 간첩행위로도 볼 수 있는데 이는 국제법의 문제로서 아래에서 다룬다. 이 단계에서의 국내법적 고려사항은 목적하지 않았던 정보를 확인하게 되는 경우로서 특히 내국인에 관한 정보를 수집하게 되었을 때라고 할 수 있다. 이 경우 관련 법적 근거 및 내부 수행지침 등을 통해 구체적인 정보관리에 관한 지침을 수립하고 목적하지 않은 내국인 정보는 삭제하고 관계가 있으나 불분명하다면 개인정보 침해 문제가 없도록 암호화하여 별도 관리하는 등의 정책을 설계할 수 있어야 한다.

한편, 국제법적 관점에서 사전 침입 및 탐지 행위가 적발될 경우 문제가 될 수 있다. 이 경우 사전 탐지 관련 가능한 항변사유로는 피해자 국적주의(수동적 속인주의), 국제사회의 공동 이익을 해하는 행위에 대한 대응으로서 보호주의, 보편주의 등 합당한 관할권 행사의 일환이었다는 주장, 국제적으로 금지되지 않은 첩보행위였다는 주장, 사안에 따라 예방적 성격의 선제적 자위권(= 예방공격)이라는 주장(이 경우 구체적 근거들이 필요할 수 있음), 또는 비국가행위자의 행위였다면 국가에 귀속되지 않는 행위이며 (확인 불가 기술 활용 등을 주장하며) 상당한 주의의무를 위반하지 않은 행위라는 주장이 가능할 것이다.

2) 사전 차단하는 행위

위협원이 공격에 착수하려고 하는 등 공격이 임박하였다면 이를 차단하는 조치가 필요할 수 있다. 이 경우 목적 달성에 필요한 수준의 조치가 이루어져야지 이를 넘어서는 과도한 결과를 야기하지 않도록 유의해야 한다. 주로 국제법상의 문제들이 있을 수 있고 국내법적으로는 관련된 시스템 등이 정보통신망법의 보호를 받는 등에 해당할 수 있다. 정보통신망법에 따르면 제48조제1항을 통해 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망을 침입하여서는 안 된다. 따라서 법률에 의한 승인이나 영장을 근거로 정보통신망에 침입하는 행위는 정당한 접근권한을 가지고 있는 것이므로 해당 규정에 저촉되지 않는다. 그러나 목적과 관계없는 시스템이 영향을 받는 때에는 이야기가 다르다. 정당한 접근권한이 아니므로 책임을 면할 수 없는 것이다. 따라서 해당 기능만을 차단할 수 있도록 면밀한 설계가 요구된다.

아울러 임박한 공격에 대한 사전 차단 행위의 경우에는 구체적 행위와 결과가 나타나게 되므로 국제법적 관점에서는 대표적으로 예방적 자위권을 주장할 수 있을 것이다. 국가책임법상 위법성 조각사유 중 긴급피난(필요성) 및 (이전의 사이버 위법행위와 예상되는 사이버 작업 사이에 일련의 연계성을 인정받을 수 있다면) 대응조치도 항변사유로 주장이 가능할 것이다. 특히 이러한 능동적 대응의 목적이 사이버조작으로 인한 피해의 효과적인 방지에 있다는 점, 그리고 사이버공간의 특성상 사후적 조치는 조치의 목적을 달성하기 어렵다는 점을 고려하면, 실제 피해가 발생하기 전이라도 피해 예방을 위한 능동적 대응을 정당한 조치로 보는 것이 타당할 것이다.

3) 공격을 받은 경우 수법과 경로를 조사해 역추적하는 행위

공격을 받아 역추적하는 경우 다양한 기관이나 민간 기업들의 협조를 받아야 할 상황이 있을 수 있다. 이 경우 민간 위협정보 공유 내지는 강제조치를 통해 신속하게 해당 정보를 획득해야 하는데 민간에 대한 개입이 결국 필수적이라는 점에서 법률적 근거가 요구된다. 역추적하는 과정에서도 불필요한 정보, 의도하지 않은 정보를 취득하게 되는 때에는 이를 즉시 삭제하는 등의 절차가 필요하다.

이러한 행위를 수행하는 과정에서는 국제적으로도 여러 주체들에 영향을 미칠 수 있다. 이 경우 상당주의의무에 따른 협조를 요청할 수도 있을 것이다. 속지주의, 피해자 국적주의, 보호주의, 보편주의 등 다양한 관할권에 근거한 주장들도 할 수 있을 것이며, 무엇보다도 자위권 행사 차원의 조치로서, 또는 만약 선행 불법행위가 무력공격에는 이르지 않은 경우에는 대응조치의 일환으로 행해진 것임을 주장할 수 있을 것이다.

4) 추적 후 보복해킹 등 비례적 대응을 하는 행위

구체적인 공격이 발견되어 이에 대한 비례적 대응을 하는 때에는 마찬가지로 주로 국제법적 쟁점이 있을 수 있고 국내법 차원에서는 앞서 지적한 바와 같이 목적 달성에 필요한 정도에 그칠 것, 나아가 제3의 무고한 시스템 등에 영향을 미치지 않을 것 등이 필요하다. 아울러 비례적 대응에 있어 정당행위 내지는 정당방위가 되려면 방위의 의사는 물론 그 행위가 지나쳐서는 안 된다. 침해의 현재성도 요구되는데 2010년 발견된 스턱스넷 공격 이후 이란의 사우디라아비아 아람코 공격, 2014년 소니 해킹 사건에 대한 일정 기간이 지난 이후의 미국의 반격 등을 고려하면 사실상 현재성은 중요한 요건이 아닌

상황이다. 그러나 법적 문제로 따지자면 분명히 요구되는 요소이므로 가능한 신속한 대응이 이루어질 필요가 있다. 한편, 국제법적 관점에서는 명백한 자위권 행사 관점에서 비무력공격 수준의 대응조치 적용을 주장할 수 있을 것이다.

2. 공세적 사이버방어 절차 및 요건 설계

1) 기본권 제한의 요건과 내용

법리적으로는 국가가 안보 목적의 정보수집 활동이나 범죄 수사목적 등의 경찰행정을 하기 위해 개인의 기본권을 침해하여야 할 경우라 하더라도 그 본질적 내용은 침해되지 못한다. 즉, 기본적으로 목적상, 형식상, 내용상 한계를 준수하여야 할 것이 요구되며 국가안전보장이라는 목적에 의해 사생활의 자유를 비롯한 프라이버시권, 개인정보자기결정권 등의 헌법적 기본권 제한의 내용을 법률로 정하여야 하고 해당 법률은 기본권의 본질적 내용을 침해하지 않아야 한다. 본질적 요소를 침해하는지의 여부는 상황에 따라 다를 수 있겠지만 그간 자유권을 통제하였던 법률을 판단하던 원칙인 과잉금지원칙 의하면, 국가안보목적의 국가행위는 정당한 목적에 따라, 적합한 수단을 통해, 기본권 침해를 최소화하고 기본권을 침해함으로써 얻게 되는 안보활동의 이익이 침해되는 개인의 기본권에 대한 침익과 균형을 이루는 법률을 형성하여야 하는 것이어야 한다. 헌법재판소는 국가권력에 의하여 개인정보자기결정권을 제한함에 있어서는 개인정보의 수집·보관·이용 등의 주체, 목적, 대상 및 범위 등을 법률에 구체적으로 규정함으로써 그 법률적 근거를 보다 명확히 하는 것이 바람직하나 개인정보의 종류와 성격, 정보처리의 방식과 내용 등에 따라

수권 법률의 명확성 요구의 정도는 달라진다 할 것이고, 일반적으로 볼 때 개인의 인격에 밀접히 연관된 민감한 정보일수록 규범 명확성의 요청은 더욱 강해진다고 한 바 있다.[42] 결국 해킹 등의 수단들이 제도적으로 허용되기 위해서는 명확한 법적 근거를 통해 프라이버시권에 대한 본질적 내용을 침해하지 않는 방법이어야 할 것이다. 온라인수색을 도입함에 있어 헌법적 한계를 제시한 판례들의 예시를 보면 독일의 경우 연방범죄 수사청법 관련 헌법소원심판[43]에서 안보분야 특히 테러 방지 목적 국가작용의 헌법적 한계를 제시하였는데, 당해 결정에서 독일 연방헌법재판소는 국제적 테러 위험 방지를 위한 연방범죄 수사청의 비밀감시권한(주거감시, 온라인수색, 통신감청, 통신자료수집과 주거 외 지역에서 특수장치를 통한 감시)은 기본적으로 연방헌법에 합치하는 것이나, 이러한 권한은 비례원칙을 충족해야 한다고 하였다. 사생활에 깊숙이 관여하는 권한은 중대한 법익의 보호를 위해서만 인정되고 그러한 법익의 위험이 충분히 구체적으로 예상됨을 전제로 하며, 감시 대상의 생활공간에 있는 제3자라 하더라도 제한적 요건에서만 감시조치의 대상이 되고, 사생활 내용의 핵심 영역 및 직업 비밀 주체의 보호를 위한 특별한 규정들이 필요하며, 투명성과 개인의 권리구제 및 감독기관의 통제를 보장해야 하고, 수집한 자료의

42) 헌법재판소 2005.5.26. 99헌마513등.

43) BVerfGE 141, 220 해당 사건은 청구인들이 동 법의 정보수집 권한(질문권, 주거내 감시, 온라인수색, 통신감청, 통신자료 수집, 개인정보수집 등)이 연방헌법 제13조 주거의 불가침, 제10조 통신의 자유, 제2조 정보시스템의 신뢰성과 불가침성을 침해하며, 수집된 정보를 다른 행정청에게 제공하거나 유럽연합 또는 국제적 협력기관에 이전하는 것이 개인정보 자기결정권 등에 위반된다며 헌법소원심판을 제기한 사건이다(정문식, "테러방지 감시조치에 대한 위헌심사기준", 「법과 정책연구」 제18집 제2호, 한국법정책학회, 2018, 7-8면.).

삭제 의무를 통한 보완이 요청된다고 하였다.[44)]

종합하여 보면, 프라이버시권 등을 포함한 개인의 사생활의 자유나 통신비밀의 자유를 제한하는 경우 해당 법률이 기본권의 본질적 요소를 침해하였는지를 판단함에 있어서 핵심적 고려 요소는 해당 행위에 대하여 법률에서 명확하게 요건과 내용을 규정하고 있는지의 여부와 그로 인해 침해되는 개인의 기본권 침해를 최소화하는 통제 방안과 구제 절차 등 절차적 방안들이 마련되어 있는지 여부, 그리고 그러한 수사권한에 대한 통제가 이루어지고 있는지 등에 대한 여부라 할 수 있다. 따라서 온라인수색에 대한 법적 허용의 출발은 허용 여부를 논하는 것에서 벗어나 이를 법률적으로 담아내는 것은 물론 이를 어떻게 통제할 것인가를 결정하는 것과 방법과 내용의 한계를 어디까지로 설정하느냐가 중요한 문제라 할 수 있다. 따라서 이러한 기준과 방법, 내용과 한계 등을 어느 정도와 범위로 수용할 것인지 입법적인 결단이 필요한 상황이다.

2) 법적 근거의 마련

사이버안보기본법 논의는 여전히 정치적 논쟁에서 벗어나지 못하고 재차 지연되는 모습을 보이고 있다. 이러한 점에서는 오히려 통신비밀보호법 개정을 통해 접근하는 방법도 고려할 수 있을 것으로 보인다.

우선 법률적으로는 예방 및 대응에 관한 일반적 기능 규정을 보다 구체적으로 설계할 수 있어야 한다. 현행 국가정보원법 제4조에 따라

44) 정문식, "테러방지 감시조치에 대한 위헌심사기준", 「법과 정책연구」 제18집 제2호, 한국법정책학회, 2018, 9면에서 재인용.

국가정보원은 사이버안보 관련 정보의 수집, 작성, 배포 및 공공기관 등을 대상으로 하는 사이버공격 및 위협에 대한 예방 및 대응 업무를 수행할 수 있다. 또한 사이버안보 관련 정보의 수집, 작성, 배포와 관련된 조치로서 국가안보와 국익에 반하는 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 활동을 확인·견제·차단하고, 국민의 안전을 보호하기 위하여 취하는 대응조치도 수행할 수 있다. 아울러 사이버안보 업무규정 제9조에 따르면 사이버공격 및 위협 예방 조치를 위해 정보화 사업의 보안성 검토, 암호장치나 정보통신기기 보안대책 수립과 검증, 정보보호시스템 개발 및 보급, 기타 보안관리 컨설팅을 수행할 수 있다. 또한 동 규정 제14조에 따라 사이버공격 및 위협을 즉시 탐지, 대응할 수 있는 보안관제체계를 구축 및 운영할 수 있다. 제16조는 사고 조사에 관한 사항을 규정하고 있으며 동조제1항에 따라 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협으로 사고가 발생한 경우 공격 주체 규명, 원인 분석 및 피해 내역 확인 등을 위한 조사를 실시할 수 있다.

이 경우 현재 예방의 관점에서는 구체적 직무가 정보화 사업의 보안성 검토 등에 한정되는 것으로 보인다. 국가정보원법에 따라 국제 및 국가배후 해킹조직 등에 관한 정보를 수집, 작성, 배포할 수 있으나 정작 이에 관한 구체적 사항은 규정되어 있지 않고 제3조를 통해 동어 반복이 이루어지고 있다. 따라서 동 규정 제9조에 항을 신설해 중앙행정기관등에 대한 사이버공격 및 위협을 예방하기 위하여 국제 및 국가배후 해킹조직 등의 동향 분석 및 위협원 식별·완화와 같은 표현을 고려할 수 있을 것이다. 또한 제16조 사고 조사를 위한 주체 규명과 원인 분석 외에도 피해의 완화나 재발방지를 위한 조치 등을 추가해 능동적 대응의 여지를 포함시킬 수 있을 것이다.

〈표 00〉 사이버안보 업무규정 개정방안

제9조(사이버공격·위협 예방 조치 등) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협을 예방하기 위하여 국제 및 국가배후 해킹조직 등의 동향을 분석하고 위협원을 식별·무력화할 수 있다. ② ~ ⑥ 생략
제16조(사고 조사 등) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협으로 사고가 발생한 경우 공격 주체 규명, 원인 분석, 피해 내역 확인, 피해의 완화 및 재발방지 등을 위한 조치를 실시할 수 있다. ② ~ ④ 생략

아울러 능동적 사이버안보 활동의 일반적 근거는 대통령령인 동 규정으로는 한계가 있고 법률 단위에서 다루는 것이 타당하다고 판단된다. 현행 국가정보원법 직무 규정에 따르면 국가정보원은 사이버안보 관련 정보를 수집, 작성, 배포할 수 있고 이와 관련된 조치로서 각종 활동을 확인, 견제, 차단하고 대응조치를 취할 수 있는데 정보의 수집, 작성, 배포와 관련된 활동의 확인, 견제, 차단, 대응이라는 규정은 사이버안보 위협에 능동적으로 대응하기 위한 근거로 활용되기에는 표현이 명확하지 못한 문제가 있다. 따라서 실제로 특정 위협에 적극적으로 대응할 수 있는 표현을 고민하여야 하는데 이러한 규정은 국방정보화법에서 잘 다루고 있는 것으로 보인다. 동법 제2조제6호에 따르면 국방정보보호란 국방정보통신망에 대한 전자적 침해행위의 거부·정지·제한·예방·대비·대응·복구·확인·점검·역추적 및 봉쇄 등 군의 작전능력을 제고하기 위한 모든 활동으로 정의된다. 이와 같은 규정을 참고해 국가정보원법의 개정 또는 사이버안보 관련 법률의 제정 시 정보통신망 침해행위의 예방, 대비, 대응, 복구, 확인, 역추적 및 봉쇄와 같은 기능을 수행하도록 할 수 있을 것이다.

〈표 00〉 국가정보원법 직무조항 개정방안

제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다. ~ 3. 생략 4. 다음 각 목의 기관 대상 사이버위협 및 공격에 대한 예방, 대비, 대응, 확인, 점검, 역추적 및 봉쇄 가. ~ 다. 생략 이하 생략

한편, 단순히 행정조직에 관한 법률에서 조직법상 기관의 권한을 부여하고 이러한 권한을 행사하기 위해 필요한 사항을 하위법령과 행정규칙에서 규정하는 것이 불가능하다고 볼 수는 없다. 문제는 실제 그 권한에 의해 행사되는 행정작용의 속성에 있다고 봐야 한다. 즉, 어떤 행정작용에 어느 수준으로 직접적, 구체적, 개별적인 수권이 요구되는지를 정할 수 있어야 하는데 여기에는 침해되는 기본권의 중요성, 침해되는 정도 내지는 수준 등을 고려해야 할 것이고 그러한 정도가 높은 행정작용이라면 더욱 구체적인 법률유보의 원칙과 포괄위임 금지 원칙이 요구된다고 할 것이다.

이러한 관점에서 세부 수행 절차는 국내 대상과 국외 대상을 구분하여 상세히 설계할 필요가 있다. 다소 내국인의 기본권을 침해할 우려가 적은 국외 정보활동을 수행하기 위한 절차는 별도로 다룰 필요가 있는 것이다. 다만, 이는 가능성의 정도에 차이가 있기 때문이고 실제 통신정보활동을 수행하는 과정에서는 의도하지 않더라도 제3자의 정보를 수집할 가능성이 있으므로 이에 대한 관리감독이 있어야 함은 물론이다. 현행 통신비밀보호법상 범죄수사 목적의 감청과 국가안보 목적의 감청 절차가 각기 다른 것처럼 사이버안보 활동에 있어서도 국내 주체를 대상으로 하는 때에는 법원의 영장을, 해외 주

체를 대상으로 하는 때에는 대통령 또는 기관장의 승인만으로도 진행할 수 있어야 할 것이다. 미국은 이와 같은 구분에서 나아가 해외정보감시법을 통해 국내정보 또는 해외정보 수집 여부, 내국인 또는 외국인 여부, 수집 대상의 위치, 수집자의 위치 등을 기준으로 상세하게 구분하고 있다.

이 외에도 워터링홀 기법을 역으로 이용하는 등 함정수사 형태로 사이버공격자를 찾아내는 것은 기회제공형 함정수사에 해당하기에 이를 위법하다고 보긴 어려우나, 그 요건이나 방법에 대하여 청소년성보호법상의 신분위장수사 등 함정수사와 같이 법원의 허가 등을 통해 적절한 통제를 가하는 내용의 입법을 통해 위헌성을 제거하고, 획득한 증거에 있어 증거능력에 관한 논란을 방지하여야 한다.

공격 원점을 찾아내어 보복해킹 등 비례적 대응을 하는 행위와 관련하여 특히 비례적 대응 부분에 있어서는 공격의사를 가지고 상호간의 침해를 유발하는 행위는 방위의사를 가지고 하더라도 정당방위로서 위법성이 조각되기 어려움을 유의하여야 한다.

아울러 이러한 능동적 대응행위는 국가기관 소속 관련 업무를 취급하는 자가 실행하는 것이기에 이들에 대한 면책과 관련하여 고의나 중과실로 위법행위를 하지 않는 한 형사적 처벌뿐만 아니라 징계처분에 대하여 책임을 지지 않도록 하여야 하며, 나아가 배상책임도 지지 않도록 하는 규정이 마련되어야 할 것이다. 관련하여 최근 호주는 정보활동 법체계를 전면 개편하면서 형사법 개정을 통해 동법 제474.6(7)의 방어권을 정보기관으로 확대하여 감청 및 데이터 수정, 해킹 등 직무수행 과정에서 선의로 행동하고 그 행위가 직무 목적상 합리적인 때에는 형사책임을 지지 않도록 하는 내용을 포함하도록 하였다.

한편, 이와 같은 부수 제도와 규정들은 모두 근본적으로 해킹 등 디

지털 환경에 걸맞은 활동의 수행 근거를 두고 있기 때문에 설계 가능한 것이므로 우리 또한 관련 근거를 마련하는 것이 급선무라고 하겠다.

3) 사업자 협조의무와 면책 규정

능동적 사이버안보 활동을 수행하려면 통신사 및 IT 업체 등의 협조가 필수적이다. 따라서 사업자의 협조의무 규정을 구현할 수 있도록 사회적 공론을 강화하되 구체적인 정책 수단을 마련할 필요가 있다. 이는 제도 구현을 위한 강제적 조치와 제재 수단에서부터 비용의 지원이나 면책 등 협력 수단에 이르기까지 다양한 스펙트럼으로 구현할 수 있을 것이다. 다만 형사제재의 경우 과도한 규제로서 사실상 입법의 문턱을 넘기 어려울 듯하며 금전적 제재를 통해 과징금이나 이행강제금의 형태로 운영하는 방안을 고려할 수 있다. 특히 감청기기 등의 설치비용은 국가에서 지원하고 운영비용에 대해서는 사업자와 별도 협의를 통해 정하거나 정부에서 부담하는 방안이 타당할 수 있다. 무엇보다 사업자 입장에서 가장 부담이 되는 부분은 비용보다도 회사의 이미지와 법적 책임 문제라고 할 수 있다. 미국과 호주의 경우 이미 통신사 면책 규정을 두고 있는 상태다. 이를 고려해 우리나라 또한 사업자 면책과 관련된 논의, 협조비용 보상에 관한 논의를 통해 합리적인 정보체계를 갖출 수 있어야 할 것이다. 아울러 이러한 면책 규정은 협조하는 관계자는 물론 실제 관련 작전을 수행하는 관계자에게도 적용되어야 함은 물론이다.

3. 신뢰성 확보 방안 설계

1) 자료관리 규정 도입

능동적 사이버안보 활동과 관련된 법률 및 지침 등 내부 규정에 개인정보보호를 위한 조항과 절차들을 설계할 수 있어야 한다. 목적하지 않은 제3자의 정보가 광범위하게 수집될 수 있다는 점, 은밀하게 수행된다는 점 등을 고려하면 사생활 침해의 우려가 클 수밖에 없고 이를 최소화하기 위해서는 정보의 명확한 관리와 감독체계 등이 병행 작동하여야 한다. 먼저 원칙적으로 목적과 무관하게 수집된 자료는 즉시 삭제할 필요가 있다. 추가적으로 해당 자료도 활용할 필요가 있다고 판단되면 긴급 여부 등을 고려하여 자료를 확보해두고 사후 조치로서 즉시 감독기관의 승인을 받도록 하는 방안을 설계하여야 한다. 필요한 자료만 남겨둔 단계에서도 목적 달성과 관계없는 정보 또는 무관한 제3자가 포함된 경우 해당 통신 내용은 삭제하거나 비식별 처리하는 등의 보호조치들이 이루어져야 한다. 이와 함께 내국인, 외국인 및 목적과 관계없는 정보 등 속성과 관계없이 모든 취득자료에 대해서는 인가되지 않은 접근이나 유출 등이 없도록 권한관리, 보안조치 등 기술적, 관리적, 물리적 보호조치들이 취해져야 한다.

2) 오남용 감독체계 수립

자료관리를 바탕으로 오남용 문제가 없는지 확인할 수 있는 감독체계의 도입이 요구된다. 이를 위해 가장 먼저 직접적으로 실질화되어야 하는 부분은 정보기관의 내부통제 기능이다.[45] 우리나라 또한 내부에 변호사나 법률 전문가를 채용하여 합법성을 검토하는 등 내

45) 한희원, "국회 정보위원회의 운영과 입법방향에 대한 고찰: 미국 상하 정보위원회의 교훈을 중심으로", 「법학연구」 제54권, 한국법학회, 2014, 88면.

부 감사조직을 구비하고 있으나 구체적인 의무나 기능, 권한이 법률로 정해져 있지 않은 상황이다. 나아가 정보기관이 스스로 오남용을 통제하기 위해 자정 노력을 수행할 수 있도록 의무를 부여하지 않고 불법행위 금지의무를 다양하게 부여하고 이에 대한 처벌을 강력하게 규정하고 있는 상황이어서 도리어 부담감만을 키운 상황이라고 할 수 있다.

따라서 우선 전문성에 기반한 현장의 1차 감독체계로서 내부통제를 내실화하고 강화해야 한다. 사전 통제와 사후 감독체계가 아무리 잘 구성되어 있더라도 진행 과정에서 현장을 감독할 수 있는 실질적 수단들이 마련되어 있지 못하면 수행 과정에서의 권리 침해 발생은 방지할 수 없다. 기본적으로 수행 과정에서 법과 윤리헌장을 준수하고 인권과 성평등, 프라이버시 문제 등을 존중하면서 그러한 틀 안에서 작전을 가장 효율적이고 전문적으로 수행할 수 있도록 하는 방법이 바로 내부통제 기능이다.[46] 작전이 진행 중일 때 오남용이 발생하지 않도록 하고 완전히 종료되지 않더라도 수시로 특정 작전 행위가 종료될 때마다 주기적으로 검토할 수 있는 방법이다. 이는 결국 가장 근본적이고 본질적인 수단으로서 사전, 사후 통제가 아무리 잘 갖춰져 있더라도 진행 과정에서 문제가 발생하지 않도록 하는 방법이다. 즉, 오남용으로 인해 발생할 수 있는 피해를 가장 빠르게 식별, 인지하고 작전을 중지시키거나 지연함으로써 피해를 신속하게 완화할 수 있는 기능을 수행한다. 이 경우 내부 감독조직은 미국의 감사관 제도

46) Geneva Centre for the Democratic Control of Armed Forces, “Intelligence Oversight”, SSR Backgrounder Series, 2017, p. 6.

와 같이 외부의 전문가 중 대통령이 지명하고 국회가 승인하는 절차를 통해 구성하는 방안도 고려할 수 있다. 이를 통해 감독조직의 구성원은 해당 조직의 장이 직접 구성할 수 있도록 하여 독립성과 전문성을 보강할 수 있다. 아울러 내부에서는 윤리의식과 준법의식을 함양하고 내부통제가 실질적으로 이루어질 수 있도록 교육훈련을 시행하여야 한다. 이는 형식적인 교육에서만 끝날 것이 아니라 구체적인 현장의 사례에 적용해서 연계할 수 있도록 이루어져야 한다. 교육훈련은 윤리나 준법 분야뿐만 아니라 통제 및 감독의 효과성, 실질성 등을 보장할 수 있는 방법론 개발이나 연구와도 연계할 수 있을 것이다.

내부통제 체계를 실질적으로 마련한 후에는 외부의 통제기구를 설립하여야 한다. 이는 국회의 기능을 강화하는 방안도 고려할 수 있으나 앞서 본 바와 같이 국회는 관련 의원의 다른 의정활동, 고유의 전문분야, 임기제한 등의 문제로 인해 전문성이 떨어질 수밖에 없다는 필연적 한계를 갖는다.[47] 이러한 점에서는 오히려 독립적인 외부 감독기구가 더 효율적이고 실질적인 기능을 수행할 수 있다고 생각된다. 필요하다면 그러한 외부 감독기구의 위원을 임명하는 과정에 국회에서 임명하는 사람을 추가하거나 국회의 의견을 반영해 대통령이 임명하는 등 우리 환경에 맞는 방식을 택할 수 있다. 이 경우 실질적인 통제 기능을 보장하려면 대통령 직속의 독립된 행정조직으로 두는 것이 타당하다고 생각된다. 통신 감청이나 정보활동 등 관계기관은 국가정보원, 검찰, 경찰, 국군방첩사령부, 군사법원 등을 모두 포괄

47) Amy B. Zegart, "The Domestic Politics of Irrational Intelligence Oversight", Political Science Quarterly 126(1), 2011, pp. 10-17.

하기 때문에 이를 전체적으로 관장해 감독할 수 있어야 하기 때문이다.[48] 그러한 관점에서 국가인권위원회와 같은 독립적 성격을 가진 기구로 국가안보기술통제위원회와 같은 조직을 고려해 볼 수 있다. 이와 함께 외부통제기구의 정보 접근을 개선해야 한다. 감독하기 위해 기밀정보에도 접근할 수 있어야 한다. 감독을 수행하기 위한 권한과 기능은 법률이 명확히 부여해줘야 한다. 미국은 CIA에 감사관직을 두면서 그 근거를 법제화하는 것이 타당한지 검토하는 과정에서 기밀정보에 접근할 수 있는 등 실질적인 본연의 감독 기능을 적절하고 효과적으로 수행할 수 있도록 명확한 권한을 줘야 한다고 봤다.[49] 통제기구의 전문성을 높이는 것도 중요하다. 효과적인 감독을 수행하기 위해 감독기구에는 반드시 고도의 기술을 활용한 정보활동을 이해하고 검토할 수 있는 전문인력을 두어야 한다.[50] 관련 인원들은 민주적 통제절차를 이해하고 법적 전문성, 기술적 전문성뿐만 아니라 국가안보 관념과 정보활동의 중요성 등을 이해할 수 있어야 한다.[51]

또한 외부 전문통제기구, 내부 독립통제부서, 국회 통제기구가 공동으로 모여 소통, 협업, 조정할 수 있는 협의체를 정기적으로 운영해

48) 이재일, 「통신감청제도의 문제점과 개선방향」, 국회입법조사처, 2015, 34면.

49) Charles A. Bowsher, "Testimony on the Establishment of an Inspector General at the Central Intelligence Agency", GAO, 1988, pp. 7-8.

50) Sharon Bradford Franklin & Eric King, Strategies for Engagement Between Civil Society and Intelligence Oversight Bodies, New America, 2018, p. 40.

51) Grazvydas Jasutis, Teodora Fuior & Mindia Vashakmadze, Parliamentary Oversight of Military Intelligence, NATO Parliamentary Assembly, DCAF, 2020, pp. 78-80.

야 한다.[52] 이를 통해 주기적으로 최근의 이슈와 입장을 공유하고 우수한 사례를 식별하여 방법을 공유하는 것도 중요한 소통의 순기능이 될 수 있다.[53]

V. 맺음말

오늘날 사이버안보 환경은 전통적인 군사적 위협을 넘어 사회·경제 전반으로 확장되고 있다. 특히 북한, 중국 등 국가 주도 해킹 사례와 주요 기반시설 공격은 국가안보와 직결된다. 이러한 복합적 위협 속에서 단순 방어에 그치지 않고 선제적이고 능동적인 공세적 사이버방어 전략이 요구되고 있다. 사이버 위협은 불투명성, 공격 우위성, 비대칭성이라는 특징을 가진다. 익명성과 은밀성으로 인해 행위자 추적이 어렵고, 공격자는 하나의 취약점만 노리면 되지만 방어자는 모든 취약점을 관리해야 한다. 디지털 전환으로 공격 표면이 확대되며, 민간 클라우드와 공급망 취약점은 국가안보 문제로 직결된다. 따라서 억지 전략의 일환으로 공격자에게 침입 시 얻는 이익보다 손실이 크다는 인식을 주는 적극적 억지가 필요하다.

본 연구는 공세적 사이버방어 전략의 구체적 이행을 위해 공세적 사이버방어를 유형별로 구분하여 개념화하고 이에 따른 행위별 고려

52) Ibid. pp. 82-83.

53) Hans Born & Aidan Wills, Overseeing Intelligent Services, DCAF, Netherlands Ministry of Foreign Affairs, 2012, p. 20.

사항과 전반적인 제도 도입 방안을 제안하였다. 연구에 따르면 공세적 사이버방어는 위협을 단순 차단하는 것을 넘어 위협원을 탐지·식별·무력화하고 필요시 역추적·보복적 대응까지 포함하는데 유형별로는 ▲사전 침입 및 탐지 ▲사전 차단 ▲공격 후 역추적 ▲비례적 대응으로 구분할 수 있다. 이는 전략적 차원에서는 방어이지만 전술적으로는 공격적 성격을 띤다. 관련된 법적 분석을 통해 공세적 사이버방어 행위에 따른 예방적, 적극적 조치 수용 가능성을 검토한 결과 경찰법의 사전배려 원칙과 같이 위협 발생 전 개입 필요성이 강조된다는 점에서 긍정적 결론을 도출할 수 있었으나 사전 침투 시에도 내국인 정보수집 등 기본권 침해 우려가 있으므로 명확한 관리·감독 절차가 필요하다. 둘째, 영장주의 적용 문제를 살펴보면 강제집행 성격을 띠는 공세적 방어는 헌법상 영장주의와 충돌할 수 있는데 현행 통신비밀보호법과 같이 법관이든 제3의 기관이든 사전 영장주의를 도입할 필요가 있다고 보았다. 아울러 통신비밀보호법을 통해 공세적 사이버방어 활동을 수행할 수 있는지 여부도 검토하였으나 동법상 감청설비에 관한 정의의 한계, 대법원의 통신제한조치에 관한 실시간성 요구 판례로 인한 한계 등으로 해킹이 허용된다고 볼 수 없고 결국 새로운 입법이 요구된다. 셋째, 정당방위 인정 여부이다. 사이버 위협 차단이 현재성·상당성을 충족한다면 정당방위 가능성이 있으나 그 수준을 넘어서 보복적 성격을 띠면 인정이 어렵다. 특히 위법성 조각 사유에만 의존할 것이 아니라 제도의 실질적 취지를 달성하기 위해서는 관련 입법시 행위자 면책 규정이 병행될 필요가 있음을 강조하였다.

이와 관련하여 공세적 사이버방어 활동을 수행하고 있는 선진국으로서 미국, 영국, 일본의 사례를 분석하였다. 미국과 영국의 경우 국

가사이버안보전략을 통해 공세적 대응을 원칙화하고 실질적인 권한 부여 등의 문제는 별도의 사이버안보 입법을 추진하기보다는 기존 정보활동 관계 법률을 통해 운용하고 있음을 알 수 있었다. 일례로 미국은 행정명령 제12333호와 해외정보감시법, 영국은 수사권법을 통해 사실상 정보기관, 수사기관 등이 해킹을 수행하고 있다. 일본의 경우 최근 법률을 제정하고 경찰관직무집행법과 자위대법을 개정해 공세적 사이버안보 활동을 수행할 수 있도록 권한을 부여하였다.

결론으로서 본 연구는 우선 공세적 사이버방어 활동의 행위 유형별 고려사항을 정리하고 절차 및 요건 설계 방안, 신뢰성 확보 방안을 제안하였다. 행위별 고려사항으로서 우선 ① 사전 침입 및 탐지 단계는 위협 식별에 필수적이지만 내국인 정보 수집 등 기본권 침해 우려가 크므로 관리 지침과 국제법적 정당성이 요구된다. ② 사전 차단 단계에서는 공격 임박 시 필요한 조치이나 과잉 대응을 피해야 하며, 국제법적으로는 예방적 자위권·긴급피난 논리로 정당화할 수 있다. ③ 역추적은 민간 협조와 법적 근거가 필요하며 불필요한 정보는 즉시 삭제해야 한다. 국제법적으로는 자위권 행사나 대응조치로 설명 가능하다. ④ 비례적 대응은 목적 달성에 필요한 범위로 제한되어야 하며 제3자 피해를 방지해야 한다. 정당방위 인정 여부와 신속한 대응이 중요하다. 아울러 절차 및 요건 설계와 관련하여 우선 기본권 제한 요건이 핵심임을 강조하였다. 헌법상 사생활의 비밀을 제한하려면 법률적 근거, 비례성, 최소침해의 원칙, 권리구제 절차 구현 등을 충족해야 한다. 이어서 명확한 법적 근거 마련이 시급하다. 현행 국가정보원법과 사이버안보업무규정은 추상적 표현에 그쳐 적극적 대응을 뒷받침하기 어렵다. 따라서 '위협원 식별·무력화', '역추적·봉쇄' 등 구체적 권한을 명문화하는 방향으로 개정이 필요하다. 셋째, 사업자

협조의무와 면책 규정이 필요하다. 통신사·IT업체 협력 없이는 원활한 정보수집 및 대응이 불가능하므로 비용 지원, 과징금, 면책 제도를 병행해 협력을 유도해야 한다. 마지막으로 신뢰성 확보를 위해 수집된 불필요한 정보는 즉시 삭제·비식별화하고, 내부통제와 외부 독립 감독기구를 결합한 다층적 감독체계를 설계해야 한다. 이를 통해 권한 오남용을 방지하고 민주적 통제를 보장할 수 있다.

〈참고문헌〉

1. 국내 문헌

국가정보원. 2022. “2022년 사이버안보 위협 주요 특징 및 내년 전망”.

김민주. 2019. “한국 사이버 보안 정책과 민간의 역할.” 한국사이버안보학회 춘계 학술대회. 서울. 5월.

김상배. 2023. “사이버 억지의 새로운 개념화: 한미 사이버안보 동맹론의 성찰적 맥락에서”, 『국제정치논총』 제63집 제2호, 한국국제정치학회.

김성돈. 2018. 『형법총론(제5판)』, SKKUP.

김소정. 2023. “2023 미국 사이버안보 전략 주요내용과 한국에의 시사점”, 『INSS 이슈브리프』423호, 국가안보전략연구원.

스티븐·제임즈. 2019. “소셜미디어의 출현과 허위조작정보의 확산.” 『사이버 공격 이론』 5집 1호, 75-101.

대법원 1996. 9. 6. 선고 95도2954 판결.

대법원 2000. 3. 28. 선고 2000도228 판결.

대법원 2016. 10. 13. 선고 2016도8137 판결.

대법원 2023. 4. 27. 선고 2020도6874 판결.

문가영. 2023. “활개치는 랜섬웨어, 전시엔 핵무기 될 것”, 매일경제 2023.09.12. https://www.mk.co.kr/news/economy/10828014.

박종재·이상호. 2017. “사이버 공격에 대한 한국의 안보전략적 대응체계와 과제”, 『정치정보연구』 제20권 제3호, 한국정치정보학회.

손효현·김동희·김소정. 2022. “사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구: SBOM 정책 추진 사례를 중심으로”, 『디지털융복합연구』 제20권 제2호.

연합뉴스. 2015. “美 F-35 전투기 설계정보, 중국 스파이가 빼돌려”, 2015.01.19. https://www.yna.co.kr/view/MYH20150119018500038

유동열. 2021. “북한의 사이버 위협 실태와 대응”, 『전략연구』 제28권 제3호, 한국전략문제연구소.

윤정현. 2019. “인공지능과 블록체인의 도입이 사이버 안보의 공·수 비대칭 구도에 갖

는 의미”, 『국제정치논총』 제59집 제4호, 한국국제정치학회.
이기춘. 2018. “독일 경찰질서행정법상 위험방지론과 리스크대비론의 현대적 변화에 관한 연구”, 『법학논고』 제62집, 경북대학교 법학연구원.
이상호. 2025. “사이버 공격에 대한 적극적 억제 능력 확보 필요성 연구”, 『국가정보연구』 제18권 제1호, 한국국가정보학회.
이재상·장영민·강동민. 2019. 『형법총론(제10판)』 박영사.
이재일. 2015. 『통신감청제도의 문제점과 개선방향』, 국회입법조사처.
이해원. 2018. “영국의 사이버 안보 법제 변천 과정 및 시사점”, 『법학연구』 제26권 제4호, 경상대학교 법학연구소.
장노순. 2016. “사이버 안보위협과 사이버 방첩의 역할과 전략”, 『국가정보연구』 제9권 제2호, 한국국가정보학회.
장노순·한인택. 2013. “사이버안보의 쟁점과 연구 경향”, 『국제정치논총』 제53집 제3호, 한국국제정치학회.
정문식. 2018. “테러방지 감시조치에 대한 위헌심사기준”, 『법과 정책연구』 제18집 제2호, 한국법정책학회.
최영훈. 2023. “국가안보실, 사이버 안보 점검…’선제적 방어 강화 노력’”, 이투데이 2023.11.15. https://www.etoday.co.kr/news/view/2302691
한희원. 2014. “국회 정보위원회의 운영과 입법방향에 대한 고찰: 미국 상하 정보위원회의 교훈을 중심으로”, 『법학연구』 제54권, 한국법학회.
헌법재판소 2005.5.26. 99헌마513.

2. 국외 문헌

Amos Toh, Faiza Patel and Elizabeth Goitein, “Overseas Surveillance in an Interconnected World”, Brennan Center for Justice, 2016.
Amy B. Zegart, “The Domestic Politics of Irrational Intelligence Oversight”, Political Science Quarterly 126(1), 2011.
Anthony D. Glosson, “Active Defense: An Overview of the Debate and a Way Forward”, Mercatus Working Paper, Mercatus Center at George

Mason University, Arlington, VA, 2015.

Berelson, Bernard R., Paul F. Lazarsfeld, and William McPhee. 1954. *Voting.* Chicago: University of Chicago Press.

Boukals, C, "Overcoming Liberal Democracy: 'Threat Governmentality' and the Empowerment of Intelligence in the UK Investigatory Powers Act". Studies in Law, Politics, and Society, Emerald Publishing Limited, 2020.

Charles A. Bowsher, "Testimony on the Establishment of an Inspector General at the Central Intelligence Agency", GAO, 1988.

Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment", Journal of Strategic Studies 36(1), 2013.

Eric Tucker, "North Korea Internet outage in wake of Sony attack over", 2014.12.23. AP, https://apnews.com/united-states-government-general-news-34ad411e0c9945a6a1d608ef54e988cf

Geneva Centre for the Democratic Control of Armed Forces, "Intelligence Oversight", SSR Backgrounder Series, 2017.

Grazvydas Jasutis, Teodora Fuior & Mindia Vashakmadze, Parliamentary Oversight of Military Intelligence, NATO Parliamentary Assembly, DCAF, 2020.

Hans Born & Aidan Wills, Overseeing Intelligent Services, DCAF, Netherlands Ministry of Foreign Affairs, 2012.

Intelligence and National Security Alliance, Cyber Intelligence: Setting the Landscape for an Emerging Discipline, INSA Cyber Intelligence White Paper, 2011.

Michael N. Schmitt et al.(eds.), TALLINN Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

Nicole Perloth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back", 2012.10.23. The New York Times, https://www.nytimes.

com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures", Stanford Journal of International Law, Vol. 50, Issue 1, 2014.

Shannon Vavra, "Cyber Command, Microsoft take action against TrickBot botnet before Election Day", 2020.10.12. Cyberscoop, https://cyberscoop.com/trickbot-takedown-cyber-command-microsoft/

Sharon Bradford Franklin & Eric King, Strategies for Engagement Between Civil Society and Intelligence Oversight Bodies, New America, 2018.

Sven Herpig, "Active Cyber Defense Operations", Stiftung Neue Verantwortung, 2021.

UK HM Government, "NATIONAL CYBER SECURITY STRATEGY 2016-2021".

UK Home Office, "Equipment Interference - Code of Practice, Home Office", 2018.

US White House, "National Cybersecurity Strategy", 2023.

A Legal Study on Offensive Cyber Defense Strategy and Institutionalization

Hyun Saerom | School of Cybersecurity, Korea University

In the contemporary cybersecurity environment, threats extend far beyond traditional military concerns, encompassing the entire socio-economic sphere and directly impacting national security. Offensive cyber defense is defined as a strategy that not only blocks intrusions but also detects, identifies, and neutralizes threat actors, and, if necessary, conducts attribution, counter-infiltration, and proportional response. It can be categorized into four types: pre-emptive intrusion and detection, pre-emptive disruption, post-attack trace-back, and proportional retaliation. Strategically defensive but tactically offensive in nature, this approach raises significant legal challenges. Analysis reveals that while the necessity of early intervention is acknowledged, concerns remain regarding infringements of constitutional rights, particularly the collection of domestic personal data, requiring strict governance and safeguards. Moreover, potential conflicts with the constitutional warrant requirement and limitations of the current Communications Privacy Protection Act highlight the need for new legislation establishing ex ante authorization and ex post oversight mechanisms. The doctrine of self-defense may apply if immediacy and proportionality are satisfied, but retaliatory measures risk exceeding these bounds. Comparative cases show that the U.S. and U.K. rely on existing intelligence and investigatory laws (e.g., FISA, Executive Order 12333, Investigatory Powers Act), whereas Japan has recently amended its statutory framework to explicitly empower law enforcement and defense authorities. Ultimately, the institutionalization of offensive cyber defense requires clear statutory authorization, structured cooperation with private actors and liability protections, strict data governance, and multi-layered oversight to ensure both operational effectiveness and democratic legitimacy.

Keyword Cybersecurity, Cybersecurity Law, Active Defense, Offensive Response, Offensive Defense

* I would like to thank the professor for his useful comments in the preparation of this paper, and I would also like to thank the anonymous judges for their valuable comments on improving the completeness of the paper.