

/일시/
2023년 4월 5일(수) 오후 3시
/장소/
더 플라자 그랜드볼룸

사이버안보 라운드테이블

사이버안보 분야의 현황 및 연구

/주최/
국가정보원
/후원/
국가보안기술연구소

사이버안보 분야의 현황 및 연구

목 차

사이버안보 위협의 진화 양상 / 01

윤 민 우(가천대학교)

미국의 사이버안보전략 분석 / 05

김 동 희(국가보안기술연구소)

사이버 전환기의 패러다임 변화 모색 / 11

최 명 길(중앙대학교)

북한의 가상자산 탈취 대응을 위한 한-미 협력 고려사항 / 15

김 소 정(국가안보전략연구원)

사이버안보법의 기본개념과 과제 / 23

박 재 윤(한국외국어대학교)

사이버안보법의 제정 필요성, 주요 내용 및 향후 과제 / 33

황 창 근(홍익대학교)

사이버안보 위협의 진화 양상

윤 민 우
가천대학교 교수

◆ 최근 사이버 안보의 진화는 단순한 범죄나 테러를 넘어 미래전의 추이와도 긴밀히 관련되어 있다. 미래전은 공간적으로도 기존의 지상, 바다, 하늘이외에 우주와 사이버, 그리고 인간의 의식(perception) 영역까지 포함한 다영역(multi-domain)에서의 전쟁으로 진화하고 있다. 또한 수단의 측면에서도, 기존의 키네틱(kinetic) 폭력을 이용한 전쟁의 범위를 넘어 정보심리전, 여론조작, 선거개입, 경제적·외교적 압박 등의 비키네틱(non-kinetic) 힘의 투사를 이용한 전쟁으로까지 확장되고 있다. 더불어 미래전에는 사이버 공간을 통해 연결되는 유·무인 전투체계가 기존의 지상, 바다, 하늘공간이외에 우주공간까지도 포함하는 물리적 공간에서 동원된다. 이와 같은 유·무인 전투체계는 기존의 탱크와 자주포, 보병, 전투함정과 잠수함, 공군기, 미사일 이외에도 새로 등장하고 있는 무기체계인 드론과 무인로봇, 무인전투차량, 무인잠수정, 위성 등을 포함한다. 이밖에도 미래전은 전쟁의 승리를 위한 군사전략과 군수 등 전투지원체계, 지휘체계, 그리고 적과 아군의 전투원과 대중들에 대한 프로파간다와 사보타지, 정신전력 등의 제반문제들에 대한 혁신을 포함한다. 이와 같은 미래전과 관련된 여러 이슈들에서 사이버 안보는 핵심적 위치를 점한다. 이는 사이버 공간이 다른 전쟁 공간들(domains)을 이어주는 연결통로로서의 성격을 가지기 때문이다.

◆ 빠르게 변화하는 안보환경에서 사이버 안보의 개념과 정의 역시 변화하고 있으며 다변화하고 있다. 사이버 안보는 통상적인 의미에서 해킹과 분산디도스(distributed DDoS) 공격, 랜섬웨어 공격 등의 사이버-기술 공격위협을 지칭했다. 하지만 점차 온라인상에서의 가짜뉴스나 오정보(misinformation), 여론조작 등의 정보콘텐츠와 관련된 문제들도 주요한 위협으로 부각되고 있다. 또한 드론과 무인자동차, 로봇, 그리고 IoT 등 AI 기반의 여러 무인디바이스들이 인터넷을 통해 서로 연결되어 사이버 안보는 이와 같은 새로 등장하는 각종 무인디바이스들과 관련된 위협의 문제로까지 확장되고 있다.

◆ 이와 같은 사이버 안보 개념의 확장과 다변화는 여러 관련 개념들과의 중첩과 애매모호함을 만들어내고 있다. 정보콘텐츠와 관련된 프로파간다와 여론조작, 가스라이팅 등은 심리전(psychological warfare)과 정보전(Information warfare), 선전전(propaganda warfare), 그리고 인지전(cognitive warfare) 등의 개념들과 깊은 관련성을 가진다. 한편 인터넷상에서 무선(wireless)으로 서로 연결된 디바이스들에 대한 침해와 탈취, 무단통제는 전자전(electronic warfare)과 상당부분 겹친다. 이는 오늘날 위성과 컴퓨터, 전투기, 전투함정, 전투차량과 보병, 그리고 드론 및 무인전투체계, 지휘통제소, 데이터저장소 등이 무선통신(wireless communication)의 방식으로 서로 사이버 공간을 통해 연결되어 있는데 이 무선통신 과정에 개입함으로써 해킹 및 디바이스 오작동, 탈취 및 파괴 등 다양한 침해 위협을 현실화시킬 수 있기 때문이다. 따라서 사이버전 이 전부터 있어왔던 전자전과 개념상으로 겹친다. 예를 들면, 드론을 이용하여 와이파이(WiFi)로 연결된 스마트폰과 태블릿 등을 해킹할 수 있으며, 역시 WiFi로 연결된 프린트의 출력물을 드론을 통해 해킹하여 외부로 전송할 수도 있다. 사이버전과 전자전의 중첩성이 강화되면서 사이버전-핵전(nuclear warfare)의 넥서스 가능성도 현실화되었다. 핵EMP(Nuclear P(electro Magnetic Pulse)탄은 컴퓨터와 정보통신망 전체를 일시에 파괴

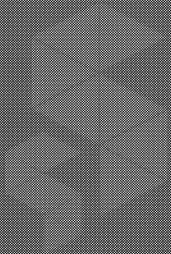
시킬 수 있는데 이는 전략적으로 오프라인에서의 폭탄투하를 통한 사이버 공간 자체에 대한 파괴의 의미를 가진다.

◆ 사이버 안보는 사이버를 구성하는 여러 개별 부문들에 대한 안보를 모두 합친 개념이다. 사이버는 ① 인터넷 기반시설과 관련 장비·부품들, ② 인터넷에 연결된 유·무인 디바이스들, ③ 디바이스들을 운영하는 운영체제(OS: Operation System)와 온라인 플랫폼(platform), 그리고 AI 등의 프로그램, ④ 가상의 네트워크 체계와 규칙들, ⑤ 인터넷 공간에서 유통되는 정보콘텐츠들, ⑥ 인터넷 공간의 정보와 인터페이스 하는 인간의 의식(perception), ⑦ 정보콘텐츠 또는 디바이스들을 연결하는 무선통신 등으로 구성되어 있다. 여기서 ①과 ②는 하드웨어로 ③과 ④, 그리고 ⑤는 소프트웨어로 정의할 수 있다. ⑥은 인간의 뇌 인지, 심리, 정서의 영역이다. ⑦은 대기(air)를 통해 연결되는 무형의 전파 또는 정보패킷(Packet), 그리고 혼합현실(Mixed Reality)의 구현 등이다. 각각의 개별부문을 보다 자세히 살펴보면 다음과 같다.

◆ 미래전은 키네틱과 비키네틱 수단이 동시에 융합적으로 동원되는 하이브리드 전쟁으로 발전하고 있다. 이는 클라우드비츠의 전쟁에 대한 고전적 정의를 다시 상기시킨다. 클라우드비츠에 따르면, 전쟁은 나의 의지를 상대방에게 관철시키는 것(enforce one's will against the other)이다. 이는 키네틱 폭력을 통해 달성될 수도 있지만 상대방의 의지(will)를 직접 개입·왜곡·조작함으로써 가능하다. 미래의 전쟁은 군사적 키네틱 결전뿐만 아니라 선거개입, 여론조작, 프로파간다, 극단주의 또는 테러리즘 유포·확산을 통한 정치사회혼란과 정부전복, 사보타지, 사이버-기술 공격을 통한 사회혼란과 공포, 경제적 압박, 전자전을 통한 정보통신네트워크의 블랙아웃, 정보전을 통한 시스템마비 등 다양한 형태로 전개될 수 있다.

◆ 미래전의 또 다른 트렌트는 인간-기계 결합살상체계(kill-chain)의 등장이다. 이는 단순히 전투현장의 전투자산에만 해당되지 않는다. 인간 지휘관들은 점점 더 AI와 같은 지능형 기계들에게 전투지휘와 통제를 위임할 것이다. 인간 지휘-명령과 기계 통제의 결합구조가 나타날 것이다. 또한 전투 현장에서 유인전투체계와 무인전투체계가 결합된 방식으로 운용될 것이다. 물론 이들 유/무인 전투체계의 전투지속성을 함께 보장하기 위한 식량과 무기, 장비, 에너지(또는 연료)의 보급과 수송, 그리고 의료와 정비체계도 중요해질 것이다. 전투현장에서 발생하는 무인전투체계의 파손을 즉시 수리하기 위한 부품 공급에 3D 프린팅 기술이 중요해질 지도 모른다.

◆ 미래전은 공격 능력의 분산, 취약성의 분산, 그리고 방어의 분산을 특성으로 한다. 국가의 정규군과 정보기관, 다른 정부부문들, 그리고 비국가행위자들을 포함한 다양한 인간-기계 공격자들의 이질적이고 비대칭(asymmetric)적인 공격역량이 분산되어 전쟁이 수행될 것이다. 취약성은 국가의 전쟁지휘부와 민간인, 정보통신기반시설과 사이버 공간에서의 여론 등 매우 다양하게 분산되어 산재할 것이다. 이처럼 공격자와 공격능력이 다양하고 취약성이 다양하고 분산되어 있기 때문에 방어역시 분산되어 운용되어야 할 필요가 있다. 따라서 공격-방어의 분산이 미래전의 특징으로 두드러질 것이다. 최근 러시아-우크라이나 전쟁에서는 이와 같은 공격-방어 분산이 나타나고 있다.



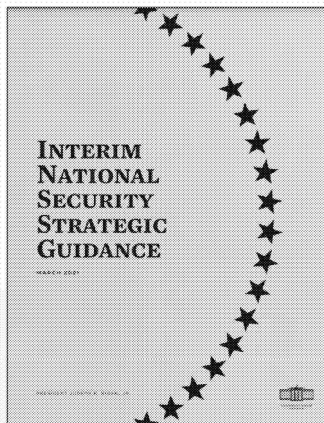
미국의 사이버안보전략 분석

2023.04.05.
김동희

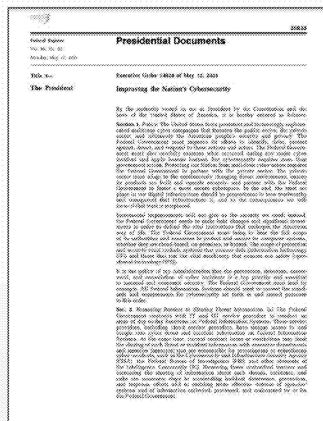
국가보안기술연구소

1. 바이든 정부의 사이버안보 정책 추진경과

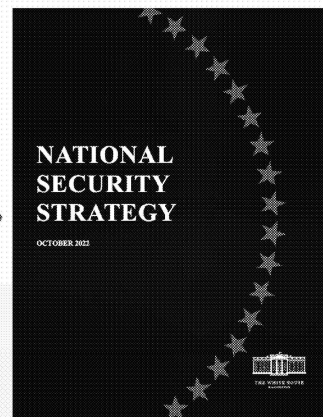
NSR



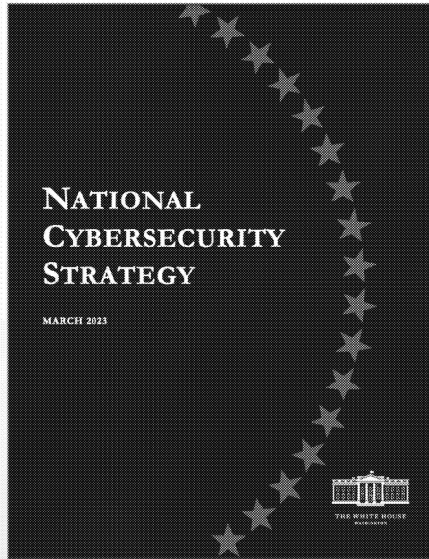
Interim National Security
Strategic Guidance
(2021.3.3.)



Executive Order 14028:
Improving Nation's
Cybersecurity
(2021.5.12.)



National Security Strategy
(2022.10.12.)



National Cybersecurity Strategy
(2023.3. 2.)

Table of Contents

- Introduction
- **Pillar 1:** Defend Critical Infrastructure
- **Pillar 2:** Disrupt and Dismantle Threat Actors
- **Pillar 3:** Shape Market Forces to Drive Security and Resilience
- **Pillar 4:** Invest in a Resilient Future
- **Pillar 5:** Forge International Partnerships to Pursue Shared Goals
- Implementation

비전(Vision)

미국은 동맹 및 파트너국과 다음과 같이 디지털 생태계를 조성하고자 함

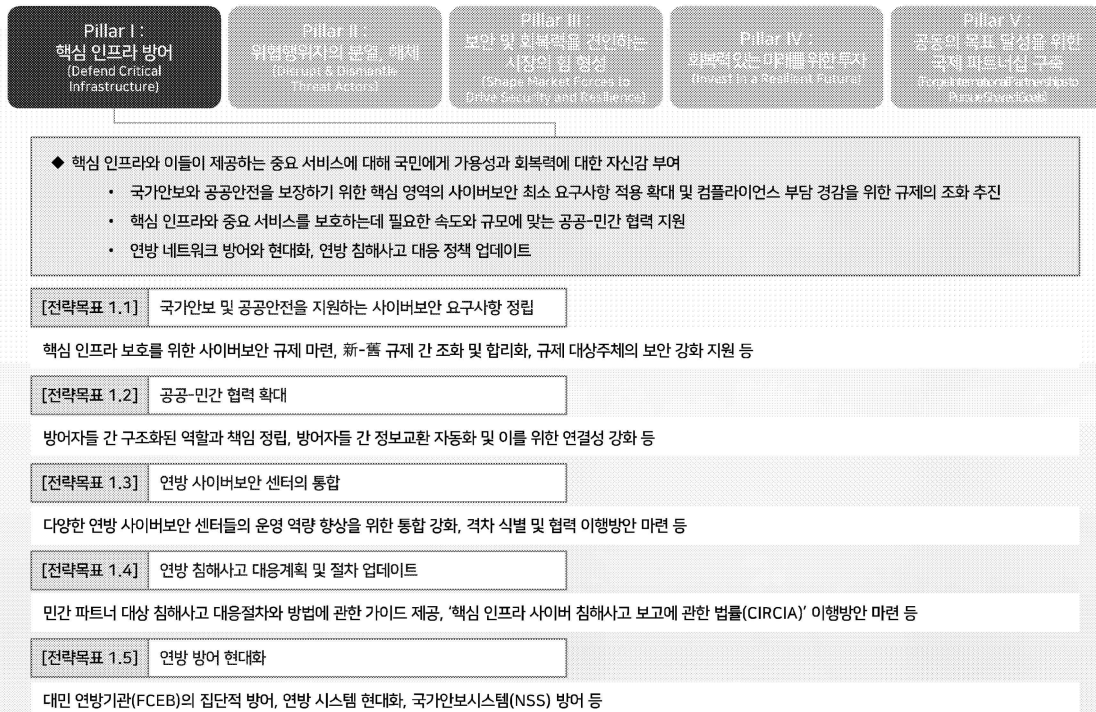
- 방어적(Defensible) : 사이버방어를 압도적으로 쉽고, 저렴하며 효과적으로 수행
- 회복적(Resilient) : 사이버 침해사고 및 오류가 광범위하거나 지속적인 영향을 거의 미치지 않도록 함
- 가치 일관적(Values-aligned) : 우리의 가장 소중한 가치가 형성되고 강화되는 디지털 세계 조성

접근법(Approach)

- 사이버공간은 미국의 국가 핵심가치인 '경제안보와 번영', '인권존중 및 자유', '신뢰할 수 있는 민주주의와 제도', '사회적 평등과 다양성'을 달성하고 이를 반영할 수 있는 중요한 수단
- 사이버안보전략에서는 이러한 사이버공간을 보호하고, 회복력을 강화하기 위한 역할과 책임, 자원 할당을 위한 다음의 2가지 근본적인 변화를 추구하고자 함
 - 사이버공간 방어를 위한 책임의 재조정
 - 장기적 투자를 위한 인센티브 조정

2. 바이든 정부의 국가 사이버안보 전략 - 5대 분야와 전략과제 (1)

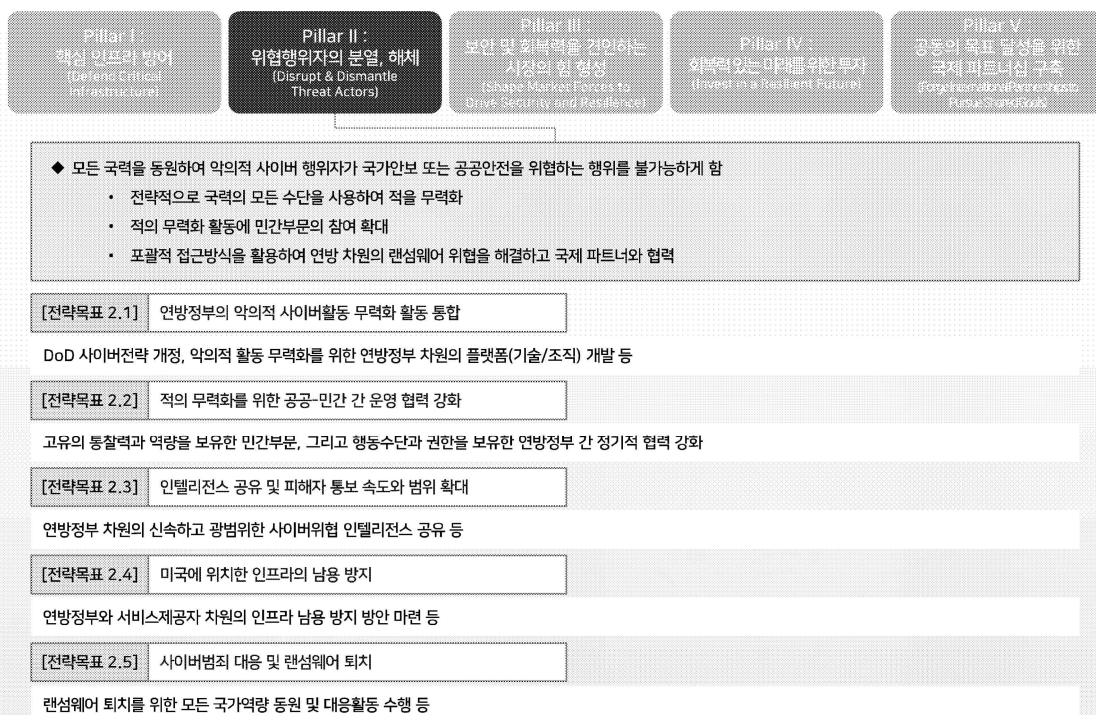
NSR



5 / 11

2. 바이든 정부의 국가 사이버안보 전략 - 5대 분야와 전략과제 (2)

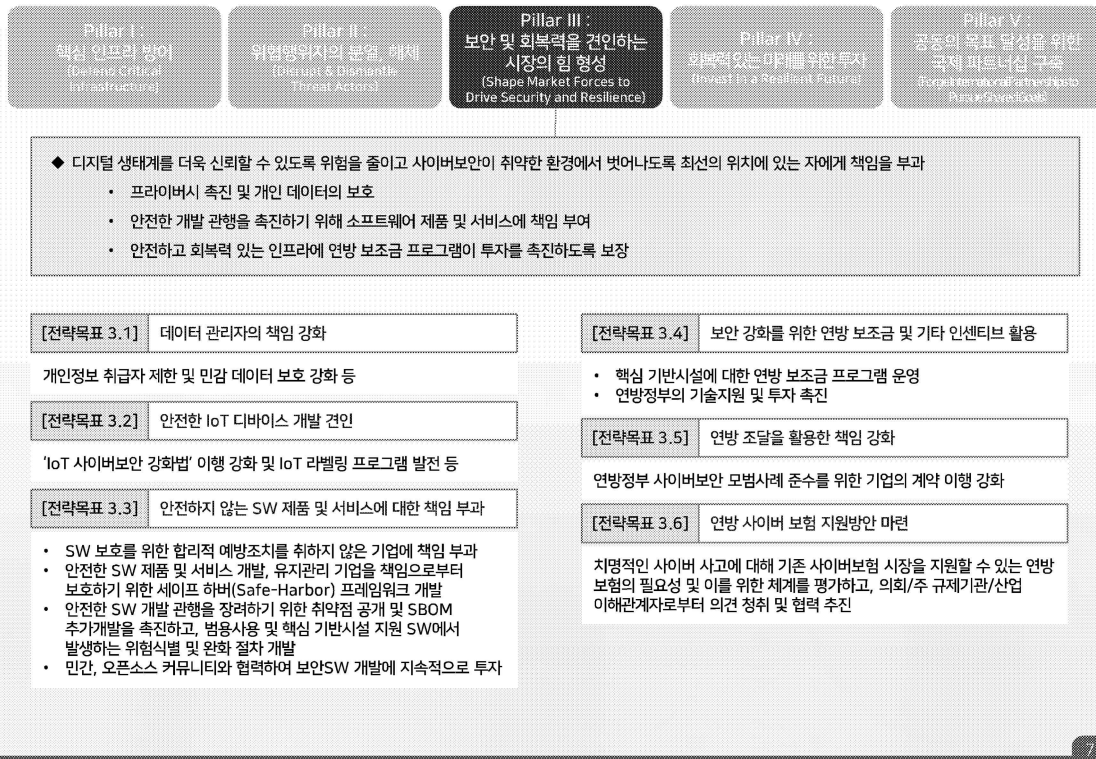
NSR



6 / 11

2. 바이든 정부의 국가 사이버안보 전략 - 5대 분야와 전략과제 (3)

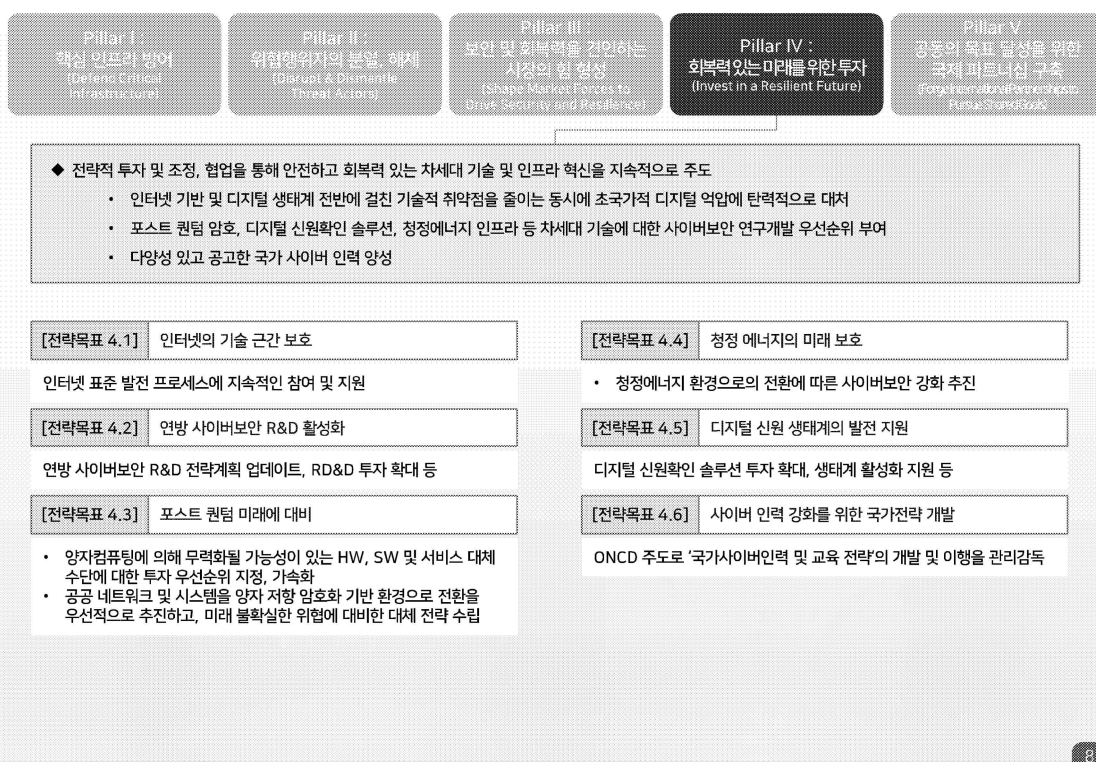
NSR



7 / 11

2. 바이든 정부의 국가 사이버안보 전략 - 5대 분야와 전략과제 (4)

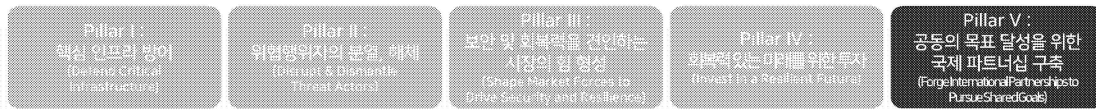
NSR



8 / 11

2. 바이든 정부의 국가 사이버안보 전략 - 5대 분야와 전략과제 (5)

NSR



- ◆ 사이버공간에서 책임있는 국가행동을 기대하고, 무책임한 행동 시 고립, 비용이 부과되는 세상을 만들어나감
 - 국제 연합과 같이 유사입장을 가진 국가들 간의 파트너십을 활용하여 공동 준비, 대응, 비용부과를 통해 디지털 생태계 위협에 대응
 - 평시, 위기 시 사이버 위협으로부터 스스로 방어할 수 있도록 파트너의 역량 강화
 - 동맹국, 파트너국과 협력하여 정보통신 및 운영 기술 제품, 서비스에 대한 안전하고 신뢰할 수 있는 글로벌 공급망 구축

[전략목표 5.1] 디지털 생태계 위협에 대응하기 위한 연합 구축

미국이 참여하는 다양한 협의회를 통해 동맹, 파트너국과 협력 강화

[전략목표 5.2] 국제 파트너 역량 강화

미국의 사이버안보 목표와 비전의 실현을 위한 유사입장국의 역량 강화

[전략목표 5.3] 미국의 동맹 및 파트너 지원 능력 확대

동맹, 파트너 국가의 중대한 사이버 침해사고 발생 시 적극 지원

[전략목표 5.4] 책임있는 국가 행동에 관한 국제규범 강화 연합 구축

적극적 외교를 통해 악의적 행위 국가에 책임을 묻고, 적대 세력을 효과적으로 억지

[전략목표 5.5] 정보, 통신, 운영 기술을 위한 제품, 서비스의 글로벌 공급망 보호

신뢰할 수 없는 외산 기업에 대한 공급망 의존도를 낮추고 공급망 재균형을 위한 국내외 공공-민간 부문의 전략적 협력 추진 등

9 / 11

3. 결론 및 시사점

NSR

미국 전략의 특징

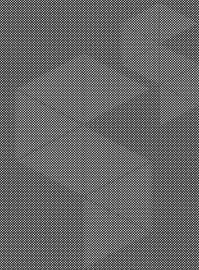
- 2018년 '국가 사이버 전략' → 2023년 '국가 사이버안보 전략'
- 국가 핵심이익 보호 등 국가안보 차원에서의 사이버공간에 대한 인식 정립 (경제번영, 인권보호, 민주주의 등)
- 자발적 표준 준수 및 협력체계 → 규제를 통한 책임을 부과하는 민관 협력 및 정부 조정의 조화 강조
- 악의적 사이버행위자 비용 부과 및 공세적 대응 기조 강화, 국내/국제 협력 강조 등

우리나라 전략 수립방향

- 국가안보의 목적과 핵심이익, 기본원칙을 반영하고 국가안보 위해(危害) 사이버공격 대응 기조 설정
- 민-관 협력에 기반하나, 필요에 따라 정부 주도와 규제를 함께 어우르는 정책 방향 제시
- 전세계적인 추세에 맞춰 능동적, 공세적 사이버위협 대응 및 이를 위한 역량 강화 방안 제시
- 전략과제의 수립, 이행결과의 검토 및 피드백이 이루어질 수 있는 평가체계 확립

10 / 11

국가보안기술연구소
| 감사합니다 |



사이버 전환기의 패러다임 변화 모색

최 명 길 (중앙대학교)

사이버 전환기의 패러다임 변화 모색

팬데믹을 기회로 보이기 시작한 사이버 전환기



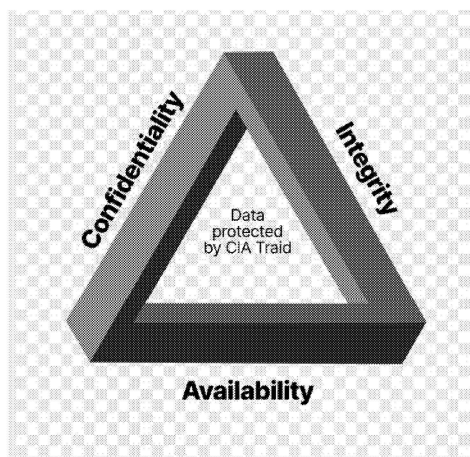
사이버 전환기의 패러다임 변화 모색

사이버 보안의 변화



사이버 전환기의 패러다임 변화 모색

보안 패러다임의 변화



사이버 전환기의 패러다임 변화 모색

추격형 기술 → 선도형 기술

Solution으로 해결 → 전방위적 해결

기술 내재 논리 → 국가, 경제 논리

수세적 논리 → 공세적 논리

사이버 공간 중심 → 4차원적 공간

패러다임 변화 모색

국가 안보와 경제 발전을 선도 가능한 사이버 정책 연구

거시 정책 환경과 기술 개발을 연결하는 사이버 기술 정책 연구

사이버 보안 연구 패러다임 체계의 근본적 변화를 주도하는 연구

사이버 전환기의 패러다임 변화 모색

북한의 가상자산 탈취 대응을 위한 한·미 협력 고려사항¹⁾

김 소 정
국가안보전략연구원

사이버공간에서 국가간 시시비비를 가릴 수 있는 명문화된 국제법은 아직 없다. 사이버공간에 적용가능한 국제법과 규범, 신뢰구축조치 등을 논의하고 있는 정부전문가그룹(GGE : Group of Governmental Experts) 회의와 개방형 워킹그룹(OEWG : Open-Ended Working Group) 회의에서도 아직 뚜렷한 성과를 내지 못하고 있다. 다만, 2015년 GGE 결과보고서는 기반시설에 대한 공격을 금지하는 11개 규범 등을 제안한 바 있다. 2022년 초 러시아-우크라이나 전쟁 개전 초기, 러시아가 우크라이나의 민간 위성 통신 시스템을 공격하여 무력화시킨 것에 대해 우크라이나 등 서방국가들은 처벌을 요구하기 보다는 민간 위성망 추가 확보를 통한 통신연결성 확보를 위해 노력했었다²⁾는 점이 아직 사이버공간을 규율하는 국제법이 존재하지 않는다는 점을 반증하고 있다. 물론, 2015년 GGE 결과보고서에서 제시한 11개 규범의 위반이라는 점에서도 러시아에 대한 비난의 근거가 되었다.

이 외에도 국제금융기구(IMF : International Monetary Fund)와 미국 썬크탱크인 카네기 엔도우먼트(CEIP : Carnegie Endowment for

1) 본 발표문은 “북한의 가상자산 탈취 대응을 위한 한·미 협력 고려사항”, 국가안보전략연구원, 「이슈브리프 395호」(2022년 10월 18일)로 출판된 원고임.

2) 김소정, “러시아-우크라이나 전쟁과 사이버안보 전략구상의 함의”, 국가안보전략연구원, 「이슈브리프 358호」, 2022년 5월

International Peace)는 금융권 기반시설에 대한 사이버공격을 악의적 행위로 규정하고, 이에 대한 공격 금지를 촉구하는 국제전략(International Strategy to Better Protect the Financial System Against Cyber Threats)를 발표했다. 또한 이를 G7 및 G20의 의제로 삼는 등 국제사회의 규범이 될 수 있도록 노력한 바 있다³⁾.

국가가 주체가 되는 공격행위와 더불어, 국가 배후 조직 및 범죄조직, 테러리스트들의 사이버공간 악용도 증가하고 있다. 2005년 이후로 34개국이 사이버 공격을 후원한 것으로 추정되며, 중국, 러시아, 이란, 북한은 의심되는 모든 공격 행위의 77%를 후원했다고 전해진다⁴⁾.

사이버공간에서 행해지는 국가주체, 혹은 국가가 후원한 단체의 행위는 국제법을 적용하는 대신, 개별 국가 주도의 사이버 범죄 대응 방식으로 처리되고 있다. 예를 들어, 지재권 탈취를 명목으로 특정 중국인들에 대한 기소⁵⁾, 수출입제한 등의 제재조치 시행⁶⁾, 공격 추정 국가 공무원 추방⁷⁾ 등으로 처리되었다. 북한 및 북한 정부의 후원을 받는 해킹조직의 가상자산 탈취 등이 지속됨에 따라 국제연합과 미국 등 주요국들이 적극적으로 대응해오고 있다. 이하에서는 북한의 사이버위협 현황과 특히 가상자산 탈취를 통한 자금원 확보, 이에 대한 미국의 노력을 살펴보고, 향후 한미간 공조를 위한 고려사항을 제시하고자 한다.

3) Tim MAURER 인터뷰, 전 카네기 엔도우먼트 프로젝트 매니저, 2019년 9월 31일.

4) <https://www.cfr.org/cyber-operations/> (최종접속 : 2022년 10월 12일)

5) 윤세미, “미국, 중국인 해커 2명 기소...사이버안보로 번지는 미중 갈등,” 아주경제, 2020년 7월 22일

6) 박수윤, “북한 '美' 사이버제재, 압박 분위기 고취 의도...북미관계 악영향”, 연합뉴스, 2022년 5월 7일

7) 황준범, “바이든, 러시아 대규모 제재 단행...“해킹 관련 외교관 10명 추방”“, 한겨레, 2021년 4월 16일

북한의 금전적 이익 보전을 위한 사이버 공격 현황

북한은 라자루스와 같은 해킹그룹을 직간접적으로 운영하면서, 이들이 해킹으로 벌어들인 외화를 새로운 자금원으로 활용하고 있다. 이를 통해 벌어들이는 불법적인 외화 규모가 상당한 금액으로 지속적으로 이뤄지고 있는 실정이다⁸⁾. 기존 북한의 대금융권 공격은 금융시스템에 대한 직접적 공격이었다. 2016년 2월 북한 해커그룹 '라저러스(Lazarus)'는 방글라데시 중앙은행이 미국 뉴욕의 연방은행에 보관한 9억5100만 달러(약 1조812억원)를 해킹했다. 해킹 공격 과정에서 실수로 인해 실제 피해액은 원래 해킹했던 금액보다 상당히 줄어든 6500만 달러(약 740억원)이었다⁹⁾. 방글라데시 중앙은행 사건처럼 기존 금융체계에 대한 해킹의 경우 시스템 침투 이후에도 돈세탁 과정을 비롯해 매우 복잡한 작업이 필요하지만, 가상화폐 시장의 탈취와 돈세탁은 이에 비해 더욱 용의하기 때문에 최근 북한의 가상자산의 탈취 및 악용은 지속될 것으로 전망된다고 전문가는 말하고 있다¹⁰⁾.

북한이 이처럼 실물 현금에 대한 공격에서 암호화폐 등 가상자산으로 그 대상을 옮기는 등 범죄자들의 최첨단 기술의 악용은 증가하고 있다. 이에 대응하는 법집행기관들도 암호화폐를 추적하여 악의적으로 탈취당한 자산을 회수하기도 했다. 실제로 FBI는 암호화폐를 추적하여 콜로니얼 파이프라인(Colonial Pipeline) 사태 당시 회사가 랜섬웨어 범죄자들에게 낸 돈의 상당 부분을 회수하는 데 성공하기도 했었다. 그래서 서로 다른 암호화폐로 변환 및 거래함으로써 추적을 힘들게 하고 익명성을 강화

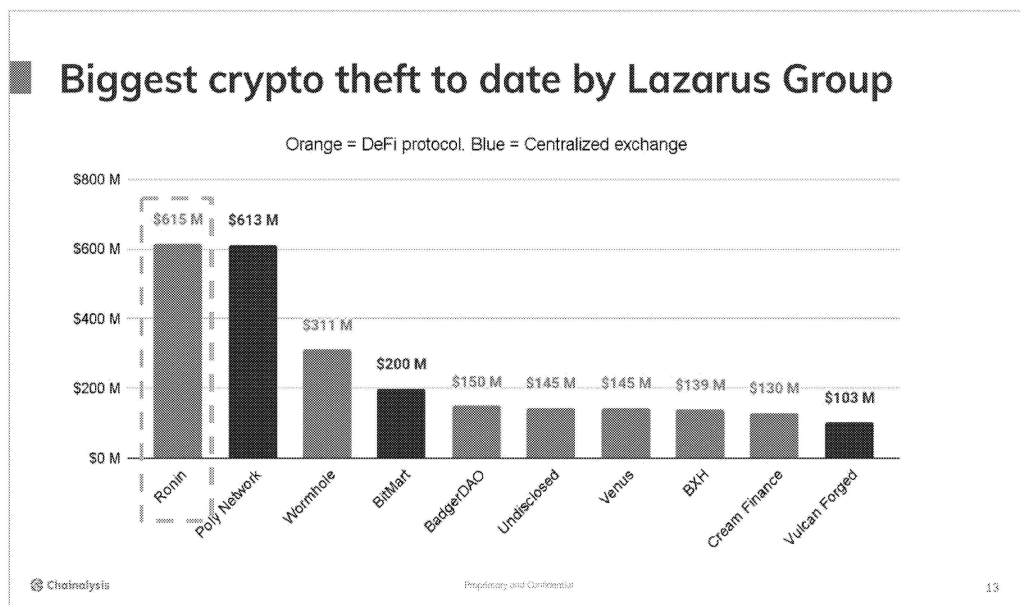
8) 이교준, “한미, 北 핵·미사일 자금줄 쫓는다..가상화폐 정조준”, YTN, 2022년 9월 11일

9) BBC, “The Lazarus heist: How North Korea almost pulled off a billion-dollar hack”, 2021년 6월 21일, <https://www.bbc.com/news/stories-57520169> (최종접속 : 2022년 10월 12일)

10) 박형주, “전문가들 “북한 '가상화폐 위협' 증가...미한 '공세적 대응' 필요”, Voice of America, 2022년 8월 10일.

하는 ‘믹서’ 서비스가 유행하기 시작했고, 북한이 이를 적극적으로 활용하고 있는 것이다.

2022년 들어, 북한의 가상화폐 자산 탈취, 탈취자산의 자금세탁, 해당 자금의 핵무기 개발 프로그램 사용이 지속적으로 언급되고 있다. 2월 발표된 블록체인 데이터 플랫폼 기업 체이널리시스의 “2022 가상자산 범죄 보고서”에 따르면, 2019년 이후 북한 연루 해킹 활동과 탈취 자금이 지속적으로 증가했으며 2017~2021년간 49차례 해킹을 통해 탈취한 자산 중 아직 세탁하지 않은 가상자산이 1억 7000만 달러라고 파악했다¹¹⁾. 라자루스 그룹에 의한 가상자산 탈취 현황은 다음의 [그림 1]과 같다¹²⁾.



[그림 1] 북한 라자루스 그룹에 의한 가상자산 탈취 현황

11) <https://www.blockmedia.co.kr/archives/212209>

12) Thomas de Zoete, "Countering proliferation with blockchain intelligence : A DPRK (Lazarus Group) case study", GCPR 2022 발표자료, 2022년 9월 20일

미국의 북한 가상자산 탈취 대응 현황

법집행기관들과 각국 정부는 암호화폐를 추적하고, 이의 불법적 활용을 저지하고자 다양한 노력을 기울이고 있다. 미국은 전세계 은행·기업에서 13억달러(약 1조4000억원) 이상의 현금 및 가상화폐를 빼돌리거나 요구한 혐의로 북한 해커 3명을 기소했다¹³⁾. 미 검찰은 북한인 3명 기소 시, 2017년 5월 파괴적인 랜섬웨어 바이러스인 워너크라이를 만들어 은행과 가상화폐 거래소를 해킹하는 등 관련 음모가 광범위했으며, 2017년 슬로베니아 기업에서 7500만달러, 2018년 인도네시아 기업으로부터 2500만달러, 뉴욕의 한 은행으로부터 1180만 달러를 훔치는 등 가상화폐 거래소를 겨냥했고, ‘크립토뉴로 트레이더’라는 앱을 침투경로로 사용했다고 밝혔다¹⁴⁾.

2월 개최된 유엔 안전보장이사회 산하 대북제재위원회에서 공개된 전문가패널 보고서는 북한이 2019년부터 2020년 11월까지 3억1640만달러(약 3575억원) 상당의 가상자산을 훔쳤다고 전했다. 북한은 훔친 가상화폐를 중국 소재 비상장 가상화폐 거래소들을 통해 실제 화폐로 바꾸는 돈 세탁하고, 탈취한 가상화폐를 핵무기 및 미사일 프로그램 개발에 사용한 것으로 추정하고 있다¹⁵⁾. 미국 사이버·신기술안보 부보좌관인 Anne Neuberger는 북한이 탈취한 금액의 1/3 이상을 미사일 프로그램 지원에 사용하고 있는 것으로 추정했다¹⁶⁾. 또한 북한이 암호화폐 거래소를 공격

13) 세계일보, “美 법무부 “北 정찰총국 해커 3명 1조4000억원 해킹 혐의 기소”, 2021년 2월 18일

<https://post.naver.com/viewer/postView.naver?volumeNo=30743372&memberNo=15305315&vType=VERTICAL> (최종접속 : 2022년 10월 12일)

14) 세계일보, “美 법무부 “北 정찰총국 해커 3명 1조4000억원 해킹 혐의 기소”, 2021년 2월 18일

<https://post.naver.com/viewer/postView.naver?volumeNo=30743372&memberNo=15305315&vType=VERTICAL> (최종접속 : 2022년 10월 12일)

15) <https://www.bbc.com/news/world-asia-60281129>

16)

<https://thehill.com/policy/technology/3590126-north-koreas-increasing-use-of-crypto-heists-to-fund-nu>

해 미사일 프로그램과 무기 프로그램을 위한 자금을 조달하는 활동을 더욱 부담스럽고 위험하며 어렵게 만드는 방안들을 알아보는데 많은 관심을 기울였다고도 언급했다¹⁷⁾.

미국 재무부는 지속적으로 북한의 가상자산 탈취를 저지하기 위한 제재조치를 발표하고 있으며, 해외자산통제국(OFAC : Office of Foreign Assets Control)은 암호화폐 믹싱 서비스를 하는 ‘토네이도 캐시’의 사용을 금지시켰다. 또한 미국 출입제한을 어기고 북한에서 열린 암호화폐 관련 학술회의에 참석하고, 북한이 제재를 회피할 수 있도록 암호화폐 관련 지식을 제공하고자 했던 미국인에 대해 징역형을 선고하기도 했다¹⁸⁾.

북한 가상자산 탈취 대응을 위한 한미 협력시 고려사항

지난 8월 미국의 신미국안보센터(CNAS)는 북한의 가상자산 탈취에 대응하기 위한 한미 공조 방안을 모색하는 웨비나를 개최했다¹⁹⁾. 동 웨비나에서 지난 3월 역대 최악의 가상화폐 탈취 사건으로 알려진 6억 2천 200만 달러 상당의 피해를 초래한 ‘로닌 해킹 사건’과 지난 6월 블록

kes-worries-us/

17) 조은정, “백악관 NSC 부보좌관 “북한, 해킹으로 거액 탈취…‘차단 방안’ 모색 중”, Voice of America, <https://www.voakorea.com/a/6788611.html> (최종접속 : 2022년 10월 14일)

18) https://www.voakorea.com/a/korea-korea-politics_virgilgriffith-nk-cryptocurrency/6032040.html (최종접속 : 2022년 10월 12일)

19) 필자는 동 웨비나의 한국 패널로 참가하여 다양한 의견을 제기하였으며, 이하 3개 문단의 내용은 웨비나의 주요 내용 중 일부를 재정리한 것이다.
Center for a New American Security, “U.S.-ROK Strategy for Enhancing Cooperation on Combating Cyber-enabled Financial Crime”, 2022년 8월 9일

<https://www.cnas.org/events/virtual-event-u-s-rok-strategy-for-enhancing-cooperation-on-combating-cyber-enabled-financial-crime> (최종접속 : 2022년 10월 12일)

체인 플랫폼인 ‘하모니 브릿지’에서 약 1억 달러 상당의 암호화폐가 탈취된 해킹 사건 모두 북한 해커들의 소행이 확실하다는 주장이 제기되었다.

동 웨비나에서 제기된 한미간 협력 방안으로 미국은 “북한의 사이버 기반시설을 겨냥하고 관련 역량을 파괴함으로써 북한 측의 사이버 작전을 방해하는 ‘공세적인 대응 작전’과 북한 해커들이 탈취한 자금을 회수하는 ‘해킹 대응(counter-hacking) 작전’에서 한미 공조 활성화”와, “북한의 기존 법정화폐(fiat currency) 돈세탁 네트워크와 관련해 두 나라가 보유한 정보를 공유·결합”을 제안했다.

한국측은 “한미 사이버 실무그룹이 북한의 가상화폐 탈취와 관련해, 관련 금융체계의 역할과 취약점, 애로사항과 문제점 등 민간 영역에 대한 이해를 출발점으로 삼는 것이 필요하”며, “한미 사이버 워킹그룹이 북한의 사이버 역량 평가와 위협 분석 등과 관련한 공동 보고서를 발간하고 북한의 관련 활동과 자금원, 자금 사용처 등을 확인하며 이에 대한 제재 이행 방안 등을 수립하는 것도 실무그룹의 역할”이 될 수 있을 것이라고 제안했다.

국내 가상자산 탈취 대응을 위한 활동은 암호화폐 등 가상자산 전문가들과 실제 금융전문가들간 교집합이 부족한 상황이다. 그리고 민간 금융권의 경우 주요기반시설로 일부 국가차원의 특별한 보호대상이 되고 있긴 하지만, 민감한 개인정보가 다수 보유되어 있다는 점에서, 아무리 공격 주체가 북한이라 할지라도 국가안보적 시각을 동반한 수사 및 조사에 예민할 수 밖에 없다. 가상자산에 대한 탈취를 위해서는 기존 금융권에서의 악의적 행위 대응 활동을 선제적 이해가 선행되어야 한다는 현실을 반영해야 한다. 또한 한미간 북한 사이버 역량, 위협 평가 등에 있어 공통의 시각을 갖고, 상호간 이해에 기반한 협력이 가능하도록 하는 환경 구축이 우선시되어야 한다.

한미 정상회담 후 한미간 워킹그룹 조직, 가상자산 탈취 등 북한의 사이버 위협 대응을 위한 공동노력은 사이버공간의 규제에 있어 많은 문제를 제기하고 있어, 정책 대응에 많은 주의가 요구된다. 한미간 북한의 가상자산 탈취 대응시 다음과 같은 사항에 대한 주의가 필요하다²⁰⁾. 첫째, 익명성이 전제되는 환경에서 법집행기관들은 실물자산이 아닌 가상자산에 대한 피해 발생시 조사 및 추적, 환수 등 조치에 어려움을 겪고 있다는 현실에 대한 자각이 필요하다. 둘째, 미국측에서 보면, 북한 관련 정보 수집에 있어 언어와 문화적 특수성으로 인한 어려움이 존재하므로 한국측 정보 의존도가 높아질 수 밖에 없다는 점을 인식해야 한다. 사이버공간에서 갖는 정보우위는 한 번 공개하면 이후에는 그 효과가 급속히 반감되는 공개의 딜레마가 있으므로, 정보공유 및 협력의 방향과 방식 결정에 신중해야 할 것이다. 셋째, 경제 제재조치를 우회한 사이버공격 및 자산탈취는 국가간 협의에 따른 제재조치의 유효성에 대해 의문을 제기할 수 있으므로 효과적인 대응조치 개발의 창의성이 요구된다. 앞으로 국제사회에서 악의적 행위자 및 행위국가에 대한 국제사회의 대응 방식에는 우크라이나나 러시아발 사이버공격 대응에 사용했던 기술적 특성을 참고한 사례도 대안으로 고려해 볼 수 있을 것이다²¹⁾.

20) 하기 고려사항은 아래 내용에 제기한 문제점을 재정리함

김소정, “가상자산 탈취 대응의 사이버안보적 함의”, 포크텍 융합문명연구원, 「코리아 리포트 10호」, 2022년 10월

21) 도메인네임 만기에 이른 러시아 웹사이트의 인증서 갱신 거부는 실제로 일어났었고, 러시아 내 제어시스템에 사용되고 있는 미국 및 서방국가들의 제품에 대한 업데이트 및 패치 거부 등이 앞으로 민간에서 시행가능한 제재에 해당한다.

김소정, “러시아-우크라이나 전쟁과 사이버안보 전략구상의 함의,” 국가안보전략연구원, 『이슈브리프 358호』 2022년 5월, p.6.

사이버안보법의 기본개념과 과제

박재윤^{**1)}

I. 문제제기

1. 政治의 司法화 > 司法의 政治화

- 과거 정당정치로 해결할 문제가 법원으로 가는 정치의 사법화가 문제되었다면, 이제 국정 전반이 법적 문제화된 후 거기서 발생한 법적 논거를 둘러싸고 정치적 논쟁이 격화되고 있음.
- 대법원과 헌법재판소의 구성은 물론 결정의 논거에 있어서도 고도의 정치적, 역사적, 학문적 논쟁이 배경이 되고 있음. 가령, 한일청구권협정의 해석과 강제징용사건, 경찰국 설치논란 등
- 정확한 법(학)적 논증을 이해하는 것이 갈등과 분쟁을 해결하는 첫걸음임.

2. 법학적 접근법이란?

(1) 기본특징

- 사실분석에서 출발하더라도 사실과 당위의 구분을 전제. (한스 켈젠 vs 칼슈미트)

1) 한국외국어대학교 교수, 법학박사, 변호사

- 엄밀한 개념정의, 규범과의 관계를 고려함.
- 실정법적 규범화를 목표로 함.
- 규범의 집행을 통한 환류과정을 가짐.

(2) 다른 학문분과에 대한 비교적 특징

- 비교법을 통하여 명확한 비교의 틀을 제공.
- 법치주의적 장치를 통하여, 법적 근거, 조직, 행위규범, 임무, 책임과 같은 조종을 할 수 있음 > 누가 언제, 무엇을, 어떻게 해야 하는지를 명확히 알려주는 것은 법의 역할임.
- 다른 학문분과의 종합적인 결과물로서 입법에 이르는 과정에서 반드시 거쳐야 하는 관문임. (소위 입법학)

3. 사이버안보의 정의와 분야의 특징

(1) 사이버 개념

- 컴퓨터를 연결하는 네트워크 망. 인터넷망, 모바일망 등을 통칭함.
- “정보통신망”이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다. (정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제1호)

(2) 사이버안보와 그 경쟁개념

- 사이버테러, 사이버공격, 사이버위협, 사이버범죄
- 사이버보안, 사이버안전, 정보보호
- 국가안보와 사이버안보

: 압도적으로 다수의 문헌이 사이버 안보란 용어를 사용. 사이버 안보는 인간의 안전을 포괄하는 개념이지만, 필연적으로 국가안보와 연결된다

는 사상을 배경으로 함.

- 사이버안보개념에 대하여, “사이버공간과 관련된 다양한 공격으로부터 국민생활과 국가안위 등을 안정적으로 유지·방어하기 위한 수단들의 총체”, “일반적으로 사이버위협으로부터 사이버공간을 보호하는 것으로, 사이버공간과 관련된 다양한 공격으로부터 국민생활과 국가안위 등을 안정적으로 유지·방어하기 위한 수단들의 총체” 등과 같이 국가안보의 개념과 비교할 때 확장적 개념이 주를 이룸.²⁾
- 2022. 11. 8. 입법예고한 「국가사이버안보 기본법 제정(안)」(이하 ‘기본법안’) 제2조 제3호도 이런 국가안보와의 필수적 관련하에서 사이버안보를 규정함. > “사이버안보”란 국제 및 국가배후 해킹조직과 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 국가안보와 국익에 반하는 사이버공격 행위 또는 활동(이하 “사이버위협”이라 한다)을 확인·견제·차단하고 이에 필요한 대응조치를 강구함으로써 국가의 안전을 보장하고 국익을 보호하는 것을 말한다.

- 개인정보와의 관계

: 개인정보는 사이버공격의 대상이면서, 사이버안보의 대응을 위하여 국가가 이를 보호하여 처리하는 수준이 문제됨. 기본법안 제16조(개인정보 처리 등) 정부는 사이버안보를 위하여 개인정보를 처리하는 경우 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리와 적절한 처리를 위하여 필요한 조치를 하여야 한다.

(3) 사실 정보 우선의 정책분야?

- 기존 법학분야에 비하여 접근이 매우 어려운 은밀한 사이버 공격기술이 문제됨.
- DDoS, TOR, APT, StuxNet 등 다양한 해킹 기술과 용어에 대한 이해가 필요함.

2) 김도승, 사이버안보 법제의 입법 동향과 향후 과제, 과학기술과 법 제12권 제1호, 2021. 6, 17면.

- 국내외 주요 사이버 공격사건, 법제도적 대응, 국제협력 등에 있어서 일단 수많은 최신 정보획득 자체가 일차적인 배경지식이 되는 분야임.
- 역설적으로 학문적 접근에 있어서는, 사실적인 부분에서 규범적인 법학적 관점을 구분하여 법논리적으로 접근하는 것이 더욱 중요한 분야일 수 있음.
- 사실을 통한 대상인식과 규범을 통한 대응전략!

II. 사이버안보법 연구범위와 성격

1. 선행연구의 개요

- 형사법적 연구: 전통적인 컴퓨터등사용사기(형법 제347조의2) 등을 비롯하여 각종 형사법적인 범죄와 그에 대한 처벌을 중심으로 다룸.
- 국제법적 연구: 사이버공격이 국가를 넘어서서 국가의 주도 내지 책임하에 이루어지는 경우가 많으므로 이를 국제법적으로 대응방안을 연구함. 주로 국제법상의 전쟁법을 현대화하여 연구. (가령, 탈린매뉴얼) 형사법적인 국가간의 협력방안을 연구하는 경우 등이 있음. (부다페스트 협약)
- 공법적인 연구: 사이버안보법제에 관한 헌법적 원칙과 행정법적 법제의 기본적 내용, 행정조직법과 행정작용법적 차원의 접근을 다룸. 기존 정보통신법제 및 개인정보보호, AI 법제 등도 이에 포섭됨.
- 비교법적인 연구: 미국, 일본 등에 대한 비교법적 연구가 많음
- 실정법제에 대한 입법적 연구: 그동안 제안된 사이버안보관련 법안에 대한 분석
- 논리적인 순서: 논리적으로 보면 형사법 > 국제법 > 공법 > 실정법제에 대한 연구의 순서로 이어짐.

2. 고유한 법학분과 인정여부

- 소위 말법(horse law) 논란: “법학과 다른 분과를 융합하여 가르치는 과목은 전체 법질서를 비추는 것이어야 하는데(illuminate the entire law), 사이버법은 ‘말의 법’(馬法, ‘The Law of the Horse’)과 마찬가지로 로스쿨에서 별도로 가르칠 필요는 없다. (Frank H. Easterbrook) vs 사이버공간을 만드는 코드로 인하여 현실공간과 차이를 이룬다. (Lawrence Lessig)”
- Kosseff 교수는 미국 실정법체계에 중요한 흠결이 드러나는 측면으로서, (1)무결성과 가용성, (2)경제적 이익과 국가안보, (3)협력적 법, (4)장래지향적 법이라는 4가지 측면을 제시함.
- 사이버 세상의 특징 + 위협에 대한 대응으로서의 안보 > 아직 완전한 분과라고 보기는 어려우나, 기존 법학분과의 법리가 도전받는 한계지점임. (탈린매뉴얼, 국가의 기여책임...)
- 개략적으로 위험방지, 리스크규제 등을 특징으로 하는 공법적인 경찰법 + 규제법 + 헌법상 국가임무로서의 안전보장 > 사이버안보법의 분과적 특징으로 설정.

Ⅲ. 실정법체계의 변화

1. 국가정보원법의 개정과 국내법제

(1) 국정원의 임무축소, 경찰이관, 구체화

: 구 「국가정보원법」(2020. 12. 15. 법률 제17645호로 전부개정되기 전의 것, 이하 ‘구법’이라 함) 제3조 제1항은 5개호의 직무(임무)규정을 두고 있었고, “국외 정보 및 국내 보안정보[대공(對共), 대정부전복(對政府

顛覆), 방첩(防諜), 대테러 및 국제범죄조직]의 수집·작성 및 배포”에 관한 직무를 수행할 수 있도록 규정하였음.

- 행정법 원리상 조직규범상의 임무규정만으로는 법률유보원칙을 충족한 것으로 평가되기 어려워서 학계의 비판은 있었으나,³⁾ 국정원의 특수성을 반영하여 그동안 실무적으로 위법으로 판단되지는 않았음.⁴⁾ (가령, 경찰의 임무는 조직법상 국가경찰과 지치경찰의 조직 및 운영에 관한 법률 제3조에 규정하고, 구체적인 작용법상의 근거는 경찰관직무집행법에 마련되어 있음. 국정원의 활동도 행정법상 경찰작용의 일환으로 파악할 수 있음.)
- 다만, 구법 중 「국가보안법」 등에 관한 수사권에 대하여는 제16조에서 사법경찰권을 부여함으로써 구체적인 작용법적인 근거가 마련되어 있었음.
- 새로 개정된 「국가정보원법」(2020. 12. 15. 법률 제17645호로 전부개정된 것, 이하 ‘신법’)은 제4조 제1항에서 구법 제3항의 직무범위를 구체화하면서, 수사권을 폐지하고 그에 관한 정보수집·작성·배포권한으로 변경함.
- 사이버안보에 대한 직무규정 신설.⁵⁾ > 여전히 작용법적인 근거는 미비함.

3) 신옥주, 국가정보원 관계 법령의 위헌성 문제와 개선방안 연구, 헌법학연구 제25권 제4호, 2019. 12. 참조.

4) 김호정, 정보기관의 정보수집 활동과 ‘개인정보 자기결정권’ -서울중앙지방법원 2008가합40668판결 및 서울고등법원 2009나60819판결을 중심으로-, 외법논집 제39권 제1호, 2015. 2. 참조.

5) 제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.

1. 다음 각 목에 해당하는 정보의 수집·작성·배포

가. 국외 및 북한에 관한 정보

나. 방첩(산업경제정보 유출, 해외연계 경제질서 교란 및 방위산업침해에 대한 방첩을 포함한다), 대테러, 국제범죄조직에 관한 정보

다. 「형법」 중 내란의 죄, 외환의 죄, 「군형법」 중 반란의 죄, 암호 부정사용의 죄, 「군사기밀 보호법」에 규정된 죄에 관한 정보

라. 「국가보안법」에 규정된 죄와 관련되고 반국가단체와 연계되거나 연계가 의심되는 안보침해행위에 관한 정보

마. 국제 및 국가배후 해킹조직 등 사이버안보 및 위성자산 등 안보 관련 우주 정보

2. 국가 기밀(국가의 안전에 대한 중대한 불이익을 피하기 위하여 한정된 인원만이 알 수 있도록 허용되고 다른 국가 또는 집단에 대하여 비밀로 할 사실·물건 또는 지식으로서

(2) 하위법령: 2020. 12. 31. 「사이버안보 업무규정」(대통령령 제31356호) 제정

- 국가, 지방자치단체 및 공공기관만을 대상으로 함.
- 법률유보원칙상 침익적 조치의 근거로 보기는 어려움.

(3) 경찰의 「경찰관직무집행법」상 정보수집권한 확대

- 2020. 12. 22. 경집법 제8조의2(정보의 수집 등) 제1항은 “경찰관은 범죄·재난·공공갈등 등 공공안녕에 대한 위협의 예방과 대응을 위한 정보의 수집·작성·배포와 이에 수반되는 사실의 확인을 할 수 있다”고 제2항은 “제1항에 따른 정보의 구체적인 범위와 처리 기준, 정보의 수집·작성·배포에 수반되는 사실의 확인 절차와 한계는 대통령령으로 정한다”고 규정하였고, 2021. 3. 23. 대통령령 제31555호로 「경찰관의 정보수집 및 처리 등에 관한 규정」을 제정함.
- 현재 비대해진 정보경찰에 대한 비판론 확대됨.⁶⁾
- 경찰국을 통한 통제론과 논쟁으로 이어짐.
-

2. 국제협력 법제

- 부다페스트 협약 가입의향서 제출 (2022. 10.)

국가 기밀로 분류된 사항만을 말한다. 이하 같다)에 속하는 문서·자재·시설·지역 및 국가안전보장에 한정된 국가 기밀을 취급하는 인원에 대한 보안 업무. 다만, 각급 기관에 대한 보안감사는 제외한다.

3. 제1호 및 제2호의 직무수행에 관련된 조치로서 국가안보와 국익에 반하는 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 활동을 확인·건제·차단하고, 국민의 안전을 보호하기 위하여 취하는 대응조치
4. 다음 각 목의 기관 대상 사이버공격 및 위협에 대한 예방 및 대응
 - 가. 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회
 - 나. 지방자치단체와 그 소속기관
 - 다. 그 밖에 대통령령으로 정하는 공공기관
5. 정보 및 보안 업무의 기획·조정
6. 그 밖에 다른 법률에 따라 국정원의 직무로 규정된 사항
- 6) 오동석, 경찰의 정보활동과 법치주의, 아주법학 제15권 제1호, 2021. 참조.

IV. 기본법안 검토

1. 법안의 성격과 한계

- 국정원법에서 미비한 법적 근거와 국가와 민간을 아우르는 조직체제를 마련함.
- 기존 사이버안보 관련 법안에 대한 시민단체 등의 비판에 따라 상세한 조문화를 자제하고 기본법 형태로만 입법함.
- 구체적인 작용법적 권한이 부족하고, 체계가 완비되지 못함. 가령, 사이버 침해사고에 대한 조사 및 정보공유 등

2. 향후 입법과제

- 기본법 제정의 완결.
- 미비한 입법을 보완, 기존 법제와의 체계성 마련.

V. 사이버안보법의 과제

1. 실용적이면서 생성중인 종합적 법분과

- 매우 다양한 최신 법기술과 사실적인 기초지식이 필요한 분야이며, 이를 기존의 법학원리에 비추어 해석하는 작업이 필요함.
- 기존의 원리와 도그마틱이 한계상황에서 처하게 됨.
- 비교법, 국제공조, 국내 입법적으로 새로운 시도가 활발하게 이루어지므로 매우 실용성이 높은 법학 분야임.

2. 현실의 정치와 정책이 교차하는 분야

- 남북한의 대치로 인하여 그동안 국정원의 역할이 매우 주목되었으며, 수사권의 문제가 논쟁의 핵심이었음.
- 사이버안보에 대한 정책은 북한이 사실상 매우 중요한 활동을 사이버공격을 통하여 한다는 점에 착안한다면, 국정원의 정보역량을 온전하게 보전할 수 있는 중요한 방안이 될 수 있음.
- 반면, 새로운 시기에 사이버안보의 이슈가 민간과 기업, 사회 전반에 매우 파급력이 높다는 점을 고려한다면, 이에 대한 우려와 논란, 신중한 접근도 요구되는 상황임.
- 이상의 산적한 문제가 현재 국내의 사이버안보법의 학문과 실천적 과제라고 생각함.

사이버안보법의 제정 필요성, 주요 내용 및 향후 과제

황창근 (홍익대 법대)

1. 사이버안보법의 제정 필요성

- 2020년 개정 또는 제정된 국가정보원법 제4조(직무), 사이버안보 업무 규정(대통령령)은 사이버안보사무의 법적 근거로 도입되는 등 구법과 비교할 때 상당히 개선된 것으로 평가하고 있음
- 그간 사이버안보에 대한 통합적, 체계적 규율의 난점이 있어서 오랜 기간 동안 여야를 불문하고 입법의 필요성은 공감하여 많은 노력이 있었으나, 거버넌스, 권한 통제 방법 등에 대한 각론의 차이등으로 입법을 하지 못하였음
- 그러나 여전히 현행 국정원법 제4조 제4호는 공공기관에 대한 사이버 공격 및 위협에 대한 예방 및 대응으로 그 업무범위를 한정하고 있는 등 문제가 있고, 이는 사이버테러, 해킹, 정보통신기반 공격 등 민관군의 경계가 없어지는 마당에 이를 분리하여 대응하는 것은 국가안보의 목적이나 대응의 실효성 차원에서 타당하지 않다는 점에서 사이버안보 통합법의 제정이 필요함
- 법치주의 관점에서 현행 사이버안보 대응체계의 법적 근거를 분명하게 정하고, 그 내용 또한 명확하고 체계적으로 정비할 필요가 있음

2. 사이버안보법의 주요 내용 및 입법 방향

- 입법 방향은 ‘기본법 + 개별법’의 이원화체계로 하되, 개별법에서는 국방, 금융, 통신, 방송 등 개별 분야별 사이버보안 또는 안전법 제정을 유도
 - 기본법이 기존 또는 추후 신설 개별법의 일반법의 지위도 갖도록 함
- 법제의 목적은 국가안전보장은 물론, 국민의 생명·신체·재산의 안전보장까지 명문화하여 국민을 위한 입법임을 천명함으로써 법제 제정의 설득력을 제고할 수 있음. 또한 국민이 참여하는 거버넌스 구성 등의 구체적인 실현방안의 개발이 필요
 - 제정안에서는 국가안전보장 이외에 국익보호를 규정하고 있으며, 위원회 구성시 국회정보위의 추천을 두고 있음
- 수범주체에 정부, 지방자치단체, 공공기관 이외에 사업자, 국민까지 명시하여 사이버안보 이슈가 전 이해당사자의 문제임을 명시하여 개별법의 기본법의 역할을 할 수 있도록 하여야 함
 - 제정안에는 국민은 포함되어 있지 않음
- 사이버안보 사무의 조직규범으로서 지위 부여
 - 사이버안보 사무가 국방, 경찰, 개인정보 등 공공은 물론이고, 정보통신사업자의 이해관계가 복잡하게 관련되어 있는 점을 감안, 독임제보다는 합의제기관이 이해관계의 조정과 타협에 유리함
- 작용규범은 법치행정원리상 행정작용의 구체화와 명확화가 요구되지만, 기본법체계를 택할 경우에는 개별법체계 보다는 그 정도가 낮더라도 개별법을 구체화하면 가능할 것이므로 기본법은 대강을 정하고 개별법에 위임하는 방식도 무방
 - 제정안 제7조(예방·대응활동)는 그런 취지로 보이고, 구체적인 행정작용의 근거로는 부족하고 법취지에 상응하는 개별법상 행정작용의 개발 과제가 남아있음

3. 향후 입법 및 연구 과제

- 사이버안보 개별법 제정 등 도출 과제
 - 향후 어떤 개별법을 입법하고, 그 개별법에 구체적인 행정작용을 넣을지를 연구하여야 함. 예컨대 ‘예방 및 대응활동’의 구체화하여 예측가능성과 안정성을 담보하여야 함. 이는 사이버보안기술의 내용이나 외국의 입법사례를 참고하여야 함
 - 분석의 요점은 법치주의원리상 조직과 작용의 근거를 완비하고 있는지, 특히 공권력작용에 대한 통제체계에 대한 연구가 필요
- 사이버안보 법제의 연계, 운영의 과제
 - 사이버안보 관련 법제로는 국가안보법, 정보법, 재난 및 안전관리법 등 다양한 법률이 존재하는데 이를 사이버안보기본법과 어떻게 연계하고 운영할 것인지 관련 법제에 대한 전반적인 분석과 정비 필요
- 공공 분야와 민간 분야의 협력 내지 연계 과제
 - 정보통신망법, 정보통신기반법, 사이버작전사령부령, 형사법 등 사이버안보, 사이버보안을 다루는 민관군 분야와 어떻게 연계할 것인지에 대한 연구 필요
 - 사이버안보의 집행체계는 범죄수사작용을 포함한 기타 행정작용과 밀접한 관련이 있으므로 그 연계에 대한 연구 필요
- 사이버안보 과학기술계와 법학 등 사회과학의 협업 과제
 - 사이버안보법제는 발전된 과학기술의 변화를 법제에 어떻게 수용하느냐에 따라 법정책의 실효성이 좌우된다고 할 것이므로 과학기술계와 법학계의 협력이 필요
- 사이버보안법제는 외국의 연구나 법제 동향과 보조를 맞추어야 하므로 외국 연구진과의 협업이나 비교법 연구가 필요