www.kacs.ne.kr

2024 KACS SPECIAL REPORT

| 2024 KACS 스페셜리포트 |

사이버 안보 국가책략:
국제정치학의 시각

한국사이버안보학회
KACS

Contents

서 론 사이버 안보 국가책략의 서론

김 상 배 | 서울대학교 정치외교학부 교수

신 승 휴 | 서울대학교 외교학전공 박사과정

1. 사이버 안보에 대한 국가적 접근의 변화 008
2. 사이버 안보 위협의 창발(emergence) 010
3. 국가책략의 개념적 논의 012
4. 중견국의 사이버 안보 국가책략 018

제1장 사이버 안보의 국가적 대응체계 마련

김 상 배 | 서울대학교 정치외교학부 교수

1. 사이버 안보 컨트롤타워의 효과적 가동 023
2. 사이버 안보의 범부처 공조 체계 정비 028
3. 사이버 안보 분야 민관협력 체계 정비 029
4. 사이버 안보 외교의 추진체계 정비 032
5. 사이버 안보 분야 법제도 정비 034

제2장 사이버 정보공유 및 대응역량 강화

김 소 정 | 국가안보전략연구원 책임연구위원, CSIS 객원연구원

1. 사이버 정보 수집·분석 및 공유 기반 강화 041
2. 사이버공격 대응을 위한 기준 고도화 방안 043
3. 공세적 방어 역량 확보 사례와 방안 046
4. 가짜뉴스 대응, 선거개입 등 영향력 공작 대응방안 049
5. AI 도입에 따른 사회적 대응역량 강화 051

제3장 사이버 범죄 및 테러의 예방·대응 역량 제고

윤 민 우 | 가천대학교 경찰행정학과 교수

1. 사이버 범죄-테러 통합정보센터 구축 059
2. 사이버 범죄-테러 대응을 위한 수사 전문성 강화 062
3. 사이버 범죄-테러 피해에 대한 신속 지원체계 강구 070
4. 사이버 범죄-테러 기관 간 공조 강화 075
5. 사이버 범죄-테러 대응 국제협약 가입 079

제4장 사이버 안보 기술역량 강화 및 공급망 안보 확보

유 인 태 | 단국대학교 정치외교학과 조교수

1. 기술개발과 공급망 재편과 관련된 국제협력 087
2. 범국가적 공급망 사이버 안보 정책 및 대응체계 확립 091
3. 국가 사이버 안보 대응 산업·기술 역량 강화 095
4. 사이버 안보 관련 기반 기술의 전략산업화 100
5. 신흥기술에 대한 사이버 위험 관리체계 확립 104

제5장 사이버 군사전략과 동맹협력

윤 대 엽 | 대전대학교 군사학과 교수

1. 한미 사이버 동맹협력의 심화 111
2. 북핵 대응 사이버 군사전략 118
3. 사이버 상호운용성과 합동성 증진 122
4. 사이버 집단안보(Cyber Collective Security) 구축 126
5. 국방 사이버 전문인력 양성 128

제6장 사이버전 수행역량 강화와 공세적 방어

설 인 효 | 국방대학교 전략학부 교수

1. 사이버전 전략 및 전술 수행 체계와 기술 고도화 133
2. 사이버전 역량의 통합 운용과 작전 수행체계 구축 137
3. 공세적 사이버 방어 및 대응 개념 정립 140
4. 사이버전 지휘통제체계 수립 143
5. 사이버전 무기체계 개발 및 전력 체계와 핵심 기술 고도화 146

제7장 사이버 불법 활동·영향력 차단 및 사이버 기반 조성

윤 정 현 | 국가안보전략연구원 연구위원

1. 가상화폐 탈취 및 경제적 불법행위 차단 151
2. 북한의 사이버 영향공작 대응체계 마련 157
3. 대북 사이버 제재 공조체계 구축 163
4. 북한사회의 디지털 억압 실태 개선 168
5. 북한 사회의 디지털 환경 실태 진단 및 활용방안 탐색 175

제8장 사이버 안보 동맹협력 및 소다자 협력

송 태 은 | 국립외교원 국제안보통일연구부 조교수

1. 한국의 사이버 안보 역량과 협력 대상 선호도 증가 183
2. 한·미 동맹 협력 의제와 전략 186
3. 한·미·일 및 한·일 사이버 안보 협력 189
4. 인태지역 소다자 그룹과의 사이버 안보 협력 192
5. 유럽 및 NATO와의 사이버 안보 협력 195
6. 결론 200

제9장 사이버안보의 국제규범 외교 및 지역협력 외교

이 정 환 | 서울대학교 정치외교학부 교수

1. <국가사이버안보전략>과 국제규범 외교 및 지역협력 외교 205
2. 사이버안보 분야 유엔외교 208
3. 국제 사이버 규범 및 신뢰구축 형성 과정에의 참여 210
4. 사이버안보 관련 가치외교 212
5. 사이버안보 지역협력 구상 주도 및 글로벌 역량강화 지원 확대 214

제10장 사이버 안보/외교와 민관협력

차 정 미 | 국회미래연구원 국제전략연구센터장

1. 사이버안보와 사이버 안보외교의 민관협력 과제 223
2. 사이버 안보의 진화와 AI-사이버 안보 민관협력 과제 231
3. 대국민 사이버 안보 인식 제고 및 민관협력 과제 232
4. 사이버 안보 국제컨퍼런스 개최 등 글로벌 리더십 강화 및 공공외교 추진 과제 237
5. 글로벌 거버넌스 대응 차원의 민관협력 과제 238

결 론 사이버 안보 국가책략의 과제

연구진 전원

1. 국가적 대응체계 정비의 과제 244
2. 사이버 보안 국가책략의 과제 246
3. 사이버 국방 국가책략의 과제 252
4. 사이버 외교 국가책략의 과제 258

서 론
사이버 안보 국가책략의 서 론

김상배 · 신승휴

1. 사이버 안보에 대한 국가적 접근의 변화
2. 사이버 안보 위협의 창발(emergence)
3. 국가책략의 개념적 논의
4. 중견국의 사이버 안보 국가책략

서 론
사이버 안보 국가책략의 필요성

김 상 배 | 서울대학교 정치외교학부 교수
신 승 휴 | 서울대학교 외교학전공 박사과정

1. 사이버 안보에 대한 국가적 접근의 변화

○ 디지털 기술의 발달과 사이버 안보의 부상

- 디지털 기술은 막대한 경제적 혜택과 사회적 편리를 제공함과 동시에 개인의 권리, 사회적 평등과 통합, 정치제도의 안정성, 국가적 가치 등을 위협하는 다층적이고 복합적인 위험 요인이 되고 있음
  · 디지털 기술은 물리적 공간의 제약을 뛰어넘어 그 파급력을 행사하고, 복잡한 시스템을 통해 구현됨으로써 높은 취약성을 가지며, 접근의 문턱이 낮아 악의적인 활용의 위험이 큼
- 디지털 기술의 이와 같은 특성으로 인해 사이버 안보의 '기술적 구조'는 단일 국가 차원의 대응이 더는 효과적이기 어려운 조건을 더해가고 있음
- 선진국과 개도국 간 경합과 미중 패권경쟁 그리고 민주주의와 권위주의 진영 간 대립으로 상징되는 사이버 안보의 '글로벌 거버넌스 구조'

와 '지정학적 구조' 역시 갈수록 더 경쟁의 성격을 드러내는 방향으로 발전하고 있음[1)]

○ 이처럼 오늘날 디지털 기술과 사이버 안보 문제가 국가안보와 경제에 지대한 영향을 미치고 강대국 경쟁의 주요 무대로 부상하는 등 '범분야 기술 문제(cross-cutting technical issue)'이자 체제 수준에서 나타나는 '기술지정학적 위기(techno-geopolitical challenge)'가 됨에 따라 이에 대한 국가적 접근 역시 변화하기 시작함

- 특히 강대국의 틈바구니에서 생존과 번영을 모색해야 하는 중견국 또는 비강대국의 입장에서 디지털 기술과 사이버 안보는 더욱 중대한 도전이 되고 있음
- 과거 사이버 안보에 대한 국가적 접근이 특정 실무부처나 전담기관 차원의 위협 대응으로 나타났다면, 현재는 범정부적-국가적 통합 차원에서 '국가책략(statecraft)'의 대응을 필요로 하는 성격을 드러냄

○ 국가책략은 국가적 대응 역량을 강화하기 위해 대내적 차원에서 다양한 영역의 국가 하위행위자와 수단을 동원하고 대외적으로는 국제협력의 범위와 밀도를 높여가는 시도를 의미함

- 사이버 안보에 대한 국가적 접근 역시 범정부적-국가적 통합 대응의 차원에서 거시적 전략목표를 설정하고 이를 추구하는 과정에 다양한

1) 김상배, "사이버 안보의 중견국 외교: 가능성과 한계," 손열, 김상배, 이승주 공편, 『한국의 중견국 외교: 역사, 이론, 실제』 (서울: 명인문화사,2016), pp. 268-310.

정부부처와 기관 그리고 민간 행위자들의 참여를 허용한다는 점에서 국가책략의 성격을 가짐

- 사이버 안보 국가책략에 참여하는 주체가 다양해지면서 대외적 협력의 범위와 밀도도 과거에 비해 대폭 확장되고 심화하는 양상을 보이고 있음

○ 따라서 사이버 안보 국가책략은 사이버 안보의 변화에 대응하는 국가적 접근, 특히 중견국의 전략이 진화하는 과정으로 이해될 필요가 있음

- 구체적으로, 사이버 안보가 '양질전화(量質轉化)'와 '이슈연계(issue-linkage)', 그리고 '지정학(geopolitics)'의 3단계 임계점을 넘어 변화하는 양상과 이에 대한 중견국의 대응 전략이 '자강(自彊) 전략'과 '네트워크(network) 전략'의 성격을 동시에 띠며 진화하는 과정에 주목해야 함[2)]

2. 사이버 안보 위협의 창발(emergence)

○ 사이버 안보의 양질전화

- 최근 디지털 기술의 급격한 발달은 사이버 안보 위협의 양적 증가와 질적 성격의 변화를 초래하고 있음

2) 사이버 안보가 3단계 임계점을 넘어 국가안보와 직결된 위협으로 부상하게 되는 원리는 다음의 연구를 참고할 것: 김상배, 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』 (서울: 한울아카데미, 2018).

- 이는 국가 행위자에 의한 사이버 공격의 파급력이 과거에 비해 대폭 증대하는 현상을 통해 특히 두드러짐. 과거 사이버 공격이 비국가 행위자나 불량국가의 수단이었다면 현재와 와서는 강대국 간 경쟁에서도 활용되는 무력행사 방식으로 자리 잡게 됨
- 한편 비국가 행위자에 의한 사이버 범죄 및 테러 위협 역시 더욱 빈번해지고 빠르게 고도화되는 상황임. 이는 디지털 기술에 대한 개인, 기업, 국가의 의존도가 빠르게 높아지면서 초래되는 결과라 할 수 있음
- 비슷한 맥락에서 디지털 기술 기반 무기체계의 악의적-비의도적 사용도 증가하는 추세임. 특히 인공지능과 같은 디지털 기술의 도입이 무기체계의 현대화 과정에서 적극적으로 이루어짐에 따라 핵지휘통제체계나 자율무기체계 등이 사이버 위협에 더욱 취약한 상태에 놓이게 됨
- 사이버 안보의 양적 증가와 질적 변화는 방대한 양의 허위조작정보가 생산되고 확산하는 결과로 이어지고 있음. 이는 최근 주요국이 영향력 공작 위협에 더욱 심각하게 노출되는 문제와도 밀접하게 연관됨

○ 사이버 안보의 이슈연계

- 사이버 안보 위협의 양적 증가와 질적 변화는 다른 이슈와의 연계를 통해 더욱 심각한 안보 문제가 되고 있음
- 디지털 기술에 대한 인류의 의존도가 높아짐에 따라 사이버 안보는 더는 고립된 분야로 보기 어려움. 그보다는 모든 분야에 걸쳐 영향을 미치는 통로의 성격을 가짐
- 따라서 사이버 안보가 전통적인 군사안보뿐만 아니라 경제안보, 우주안보, 핵안보, 데이터 안보, 공급망 안보, 기술(시스템)안보, 사회안보 등 여타 초국적 안보 이슈와 중첩되고 연계되는 양상이 더욱 뚜렷해지고 있음

- 사이버 안보의 이슈연계는 단순히 사이버 위협의 범위가 확장되는 것을 넘어 역으로 다시 사이버 안보의 질적 성격이 변화하게 되는 요인으로 작용한다는 점에서 국가적 차원의 대응을 더욱 어렵게 함

○ 사이버 안보의 지정학

- 현재 사이버 안보의 가장 주목할 특징은 사이버 위협이 양질전화와 이슈연계의 문턱을 넘어 전통적인 안보 이슈와 만나게 되면서 지정학의 문제로 창발하게 되는 경향으로 볼 수 있음
- 기존에 비전통 안보 분야로 분류되던 사이버 안보가 오늘날 개인과 국가 그리고 국제사회를 위협하는 신흥안보로 인식되는 가장 큰 이유는 국제관계의 맥락에서 다뤄져 온 군사안보, 외교안보, 규범안보 등 전통적인 국가안보와의 결합에서 찾을 수 있음
- 군사적 혁신과 군비경쟁(군사안보 이슈), 디지털 기술을 포함한 첨단기술 분야 국가 간 안보협력과 진영 간 대립(외교안보 이슈), 디지털 기술의 효과적인 규제를 위한 글로벌 차원의 윤리규범 담론과 논의(규범안보 이슈)는 사이버 안보와 떼려야 뗄 수 없는 관계에 있음

3. 국가책략의 개념적 논의

○ 국가책략의 개념은 크게 국내적·국제적 맥락에 따라 구분되어 이해할 수 있음

- 국내적 차원에서는 국가가 목표를 설정하고 추구하기 위해 수행하는

'통치술'이자 국정운영 기술 및 역량으로 정의됨. 이는 국내정치, 안보, 경제, 사회 등 특정한 영역에서 수립·추진되는 정책보다 더 광의의 개념으로 볼 수 있음

- 국제적 차원에서는 무정부 국제체제에서 국가가 핵심 목표를 달성하기 위해 외교, 국방, 경제·무역, 과학·기술, 문화 등 거의 모든 분야에서 정책 수단을 활용하여 대외적 영향력을 표출하는 행위로 정의됨
- 다만 국가책략은 결국 국가의 생존과 번영을 위해 수행된다는 점에서 국제적 차원에서 설정되는 목표(ends)와 그러한 목표를 달성하기 위해 대내외적 수단(means)을 모두 모색하고 동원하는 시도로서 이해될 필요가 있음[3)]
  - 즉 수단과 목표를 연결하는 개념으로서 목표 달성을 위해 국가가 사용할 수 있는 전반적인 권력 수단들이 무엇이며, 그러한 수단 중 선택의 대상은 무엇인지, 그리고 그 사용의 효과를 아우르는 것임[4)]

○ 국가책략은 '대전략(grand strategy)'의 개념과 비슷하면서도 엄밀한 의미에서 차이를 가지는 개념임

- 대전략은 본래 국가의 핵심 이익을 달성하기 위해 제한된 동원 가능 자

3) Morton A. Kaplan, "An Introduction to the Strategy of Statecraft," World Politics Vol. 4, No. 4 (1952), 548-576.; Markus Kornprobst, "Statecraft, Strategy and Diplomacy," in Costas M. Constantinou, Pauline Kerr, and Paul Sharp (eds.), The SAGE Handbook of Diplomacy (London: SAGE Publications Ltd, 2016), 54-66.

4) Stacie E Goddard, Paul K MacDonald, and Daniel H Nexon, "Repertoires of statecraft: instruments and logics of power politics," International Relations Vol. 33, No. 2 (2019), pp. 304-321.

원을 가능한 한 효과적으로 조정하고 사용하는 것으로 정의됨

- 대전략의 개념은 상황에 따라 계획(plan), 지침(guiding principle), 행위 패턴(pattern of behaviour) 중 하나의 의미로서 사용된다면 점에서 국가책략과 맥이 닿는 부분이 있음
- 그러나 대전략은 또 한편으로 특정 시기 집권 세력의 정치적 성향이나 정책적 경로의존성을 떠나 지속성을 가지고 유지되는 것을 의미하기도 한다는 점에서 국가책략과는 구별해서 이해할 필요가 있음

○ '분야 중점적 책략(sector-focused statecraft)'의 의미로서 특정 분야의 특수성을 바탕으로 수행되는 전략적 행위에 주목하여 국가책략을 개념화하기도 함

- 군사책략(military statecraft), 경제책략(economic statecraft), 디지털 책략(digital statecraft)처럼 특정 분야에서 국가적 목적을 위해 그 분야와 관련한 수단을 활용하는 방법이 이에 해당함
- 분야 중점적 책략의 맥락에서 국가책략을 규정하는 시각에서는 그 수행을 위해 동원되는 '수단(instrument)'으로서 군사력이 가장 중요하다는 기존의 인식을 넘어설 것을 요구함[5)]
  · 외교가 군사력에 종속된다고 보지 않으며, 외교나 경제적 수단 또는 선전선동(propaganda)과 같은 비군사적 수단 역시 군사력만큼이나 중요하고 효과적임을 강조하는 의미가 있음

5) David A. Baldwin, "Force, fungibility, and influence," Security Studies Vol. 8, No. 4 (1999), pp. 173-183.

· 비용 측면에서는 비군사적 수단이 군사적 수단보다 더 유리한 측면이 있다고 판단할 수도 있음

- 특히 상호의존적인 관계에서 발생하는 비대칭성을 통해 상대를 억압하여 자신의 이익을 추구하는 경제책략이 지금껏 많은 주목을 받아옴

○ 전략 수행을 위한 배경을 의미하는 '전략문화(strategic culture)'의 맥락에서 국가책략을 보는 시각도 존재함

- 전략문화는 국가의 정책과 전략적 행동을 형성하는 데에 영향을 미치는 전통적인 문화적, 역사적, 정치적, 사회적 요인들의 총합을 의미하며, 여기에는 한 국가가 놓인 지속적인 외부 환경이 그 국가가 군사력을 포함한 국력을 인식하고 사용하는 독특한 방식을 결정한다고 보는 시각을 바탕으로 하고 있음[6)]

- 전략이 경쟁의 상황에서 힘을 동원하고 승리하기 위한 수단이라면, 책략은 그러한 전략이 수월하게 수립·전개될 수 있도록 환경적 요건을 마련하는 일이 됨

- 특정 지역(region)에서 공유되는 외교적 문화(diplomatic culture)나 종교적 관행을 국가전략과 연관해서 이해하는 시각 역시 이와 관련이 있음[7)]

○ '외교(diplomacy)'와 국가책략의 연관성을 강조하는 차원에서 과거 조선

6) David J. Kilcullen, "Australian Statecraft: The Challenge of Aligning Policy with Strategic Culture," Security Challenges, Vol. 3, No. 4 (2007), pp. 45-65.

7) F. Gregory Gause, III, "Sovereignty, Statecraft and Stability in the Middle East," Journal of International Affairs Vol. 45, No. 2 (1992), pp. 441-469.

책략(朝鮮策略)처럼 국제정치의 구조와 그 안에서 특정 국가가 모색해야 할 위치에 주목하여 국가책략의 개념을 사용하기도 함

- 외교책략의 관점 역시 국내정치 상황보다는 국제정치 상황을 고려하여 국제체제의 구조적 변화에 발맞춰 추진되는 국가의 행위로서 책략을 강조함
- 다만 국제체제의 구조를 어떻게 바라보는가에 따라 외교에 담긴 목표의식과 수행 방식이 달리 규정되는데, 이는 크게 두 가지로 나누어 볼 수 있음
  · 그 하나는 국제체제의 구조를 물질적 국력의 상대적 배분 상태로 이해함으로써 그러한 권력구조의 변화에 따라 주요 강대국들을 대상으로 균형(balancing)과 편승(bandwagoning)을 선택하는 방식임[8)]
  · 다른 하나는 국제체제의 구조를 관계적 맥락에서 인식함으로써 소수의 강대국뿐만 아니라 여러 다른 비강대국들과의 관계를 이해하고 조정함으로써 자신의 특수한 구조적 위치를 모색해 국익을 추구하는 '관계 중심적 책략(relationship-centric statecraft)'임[9)]

○ 상기한 개념적 정의와 논의를 종합하자면, 국가책략은 '무정부 국제체제에서 주권국가의 생존과 번영을 보장하는 기술'이나 '핵심 국익을 달성하기 위해 힘을 기르는 전략이 구축되고 실행될 수 있는 유리한 환경을

8) Kornprobst, 2016.

9) 이는 주로 네트워크 이론의 시각에서 국가전략을 분석하는 시도에서 발견됨. 이와 관련하여 다음을 참고할 것: 김상배, "네트워크로 보는 중견국 외교전략: 구조적 공백과 위치권력 이론의 원용." 국제정치논총 제51집 3호 (2011), pp. 51-77.

조성하는 방법'으로 정의될 수 있음

- 이는 쉽게 말해 '자강 전략'과 '네트워크 전략'이 혼합된 형태로서 대내적으로 국가적 역량과 경쟁력을 강화하고 대외적으로는 다른 국가들과의 관계 조율을 통해 국익을 실현해 나가는 방법임
  - · 여기서 '네트워크 전략'이란 국가가 국제체제를 여러 국가 간 관계의 총합으로 존재하는 관계구조 또는 네트워크로 인식함으로써 그 안에서 자신이 차지하거나 추구하는 구조적 위치와 역할을 모색함과 동시에 그 과정에서 주변 국가들과의 관계를 조정해 나가는 전략적 행위를 뜻함
  - · 결국 자강-네트워크 전략으로서 국가책략은 자체적 역량 강화를 위한 대내적 차원의 노력과 더불어 중개외교, 연대외교, 규범외교 등으로 나타나는 대외적 차원의 노력을 필요로 함
- 무엇보다 국가책략은 '결과물(outcome)'이 아닌 '과정(process)'이라는 점에 주목할 필요가 있음
  - · 국가책략은 정책 결과물이 아니라 국가적 목표를 설정하고 그러한 목표 달성을 위해 동원 가능 자원을 결집·배치하고 이를 토대로 적절한 수단을 활용해 나가는 과정으로 해석되어야 함
  - · 즉 국가책략은 국가를 하나의 블랙박스(black box)가 아닌 '적응하는 행위자이자 시스템'으로 봄으로써 그 적응의 과정을 분석하거나 진단하는 시도로 이해되어야 함[10)]

10) Alexander L. George, "Knowledge for Statecraft: The Challenge for Political Science and

4. 중견국의 사이버 안보 국가책략

○ 중견국의 국가책략은 네트워크적 사고에 기초한 '중견국 전략(middle power strategy)'의 시각을 적극적으로 반영함

- 중견국은 속성론, 행태론, 관계론 등의 시각에 따라 달리 정의될 수 있지만, 통상적으로 인구, 영토, 군사력, 경제력 등 물질적 능력을 기준으로 강대국이나 약소국으로 분류되지 않으며 국제정치 문제에 '잠재적으로 중요한(potentially significant)' 영향을 미칠 수 있는 국가를 의미함
- 네트워크화된 국제정치 환경에서는 복잡하게 연결된 관계망의 구도나 흐름을 자신에게 유리한 방향으로 조정하는 것이 중견국에게 무엇보다 중요함
- 관계적 맥락에서 발생하는 권력과 경쟁력을 활용할 줄 아는 국가일수록 더 효율적으로 국익을 추구하거나 영향력을 행사할 수 있다는 점에서 물질적 국력의 측면에서 열세에 놓인 중견국은 네트워크적 사고에 기초한 국가책략을 전개해 나가야 함

○ 자강-네트워크 전략으로서 중견국의 사이버 안보 국가책략은 사이버 안보 위협이 심화하고 기술지정학적 위기가 고조되는 상황에 대응하기 위해 국가가 추구해야 할 목표와 수단을 아우르는 개념으로 정의될 수 있음

- 중견국은 비강대국의 한계를 뛰어넘어 국익 실현과 국제적 영향력 확

History," International Security Vol. 22, No. 1 (1997), 44-52.

장을 위해 자강 전략과 네트워크 전략을 적절히 배합한 국가책략을 추구해야 함

○ 먼저, 자강 전략의 측면에서 사이버 안보 위협에 대한 대응 능력과 사이버 복원 능력을 끌어올리기 위해 자체적인 역량을 키우고 디지털 기술 분야 국가경쟁력을 높이는 한편,

- 그러한 국가적 차원의 노력이 효율적으로 이루어질 수 있도록 이전까지 분산되어 있던 동원 가능 자원을 규합하고 이를 효율적으로 활용하는 과제를 포함함
- 특히 범정부적 협력과 정부-민간 협력을 조율하고 강화하는 노력이 중요함
- 이는 사이버 안보 분야 국가전략의 추진체계(또는 수행체계), 법제도적 장치, 민관협력 거버넌스 등을 정비하는 과정으로 나타남

○ 네트워크 전략의 측면에서는 기술, 이념, 질서, 규범 등에 걸쳐 전개되는 강대국 간 기술지정학적 경쟁의 관계적 구도와 흐름을 명확히 포착하고 이를 바탕으로 자신의 국익이 최대한 보장될 수 있는 구조적 위치와 역할을 모색하는 노력이 요구됨

- 이는 비단 사이버 안보와 디지털 기술 분야에서 미국이나 중국 등 강대국의 이해관계와 그들 간 갈등 구도를 이해하는 것을 넘어 동 분야에서 나타나는 국제적 협력과 경쟁의 양상을 파악하는 노력을 의미함
- 그러한 맥락에서 중견국 외교의 3대 축에 해당하는 중개외교와 연대외교 그리고 규범외교를 사이버 안보 분야에서 적절히 펼쳐나가는 것이 중요함

- 구체적으로, 국가 간 갈등과 강대국 경쟁이라는 맥락에서 외교적 협력의 필요성을 지적하는 중개외교, 사이버 안보 국제규범과 글로벌 거버넌스를 형성하는 국제적 노력에 참여하거나 이를 선도하는 연대외교, 그리고 미중 간 사이버 안보 경쟁의 이면에 깔린 강대국 담론을 경계하고 대안을 제시해 나가는 규범외교를 전개하는 것을 뜻함
  · 즉 사이버 안보의 협력과 갈등 구조를 관계적 맥락에서 이해함으로써 자신의 배타적 국익뿐만 아니라 중견국으로서 추구해야 할 지역 및 글로벌 차원의 공익이 최대한 보장될 수 있는 '구조적 공백(structural hole)'과 위치를 찾아가는 '위치지성(positional intelligence)'이 요구됨

제1장

사이버 안보의 국가적 대응체계 마련

김 상 배 | 서울대학교 정치외교학부 교수

1. 사이버 안보 컨트롤타워의 효과적 가동
2. 사이버 안보의 범부처 공조 체계 정비
3. 사이버 안보 분야 민관협력 체계 정비
4. 사이버 안보 외교의 추진체계 정비
5. 사이버 안보 분야 법제도 정비

제1장

사이버 안보의 국가적 대응체계 마련

김 상 배 | 서울대학교 정치외교학부 교수

배경과 구성

- 사이버 안보 국가책략(cybersecurity statecraft)의 내용을 담은 기존 문서들, 즉 <국정과제>, <국가안보전략>, <국가사이버안보전략> 등을 검토하고 향후 사이버 안보 전략의 구체적인 실천 방향을 모색
- 특히 <국가사이버안보전략>에 이어 사이버 안보 전략을 구체화 및 이행하는 차원에서 수립 및 추진될 것으로 예정된 <국가사이버안보기본계획>과 <국가사이버안보시행계획>을 염두에 두고 구체적인 정책 논의를 펼침
- 사이버 안보의 국가적 대응체계를 마련하는 거시적 시각에서 컨트롤타워, 범정부, 정부-민간, 국제협력, 법제도 등 다섯 가지 주요 어젠다를 검토
- 사이버 안보의 국가적 대응체계를 정비하는 가시적 목표로서 다층적인 국가적 추진체계와 범정부 공조체계, 민관 협력체계, 법제도 등에 대한 논의에 초점

- 제1장의 구성은 아래와 같이 다섯 가지 항목을 중심으로 함

  1. 사이버 안보 컨트롤타워의 효과적 가동
  2. 사이버 안보의 범부처 공조 체계 정비
  3. 사이버 안보 분야 민관협력 체계 정비
  4. 사이버 안보 외교의 추진체계 정비
  5. 사이버 안보 분야 법제도 정비

1. 사이버 안보 컨트롤타워의 효과적 가동

○ 복잡하고 다양화된 사이버 위협에 효과적으로 대응하기 위해 분산된 대응체계를 개선하여 좀 더 유기적으로 작동하는 국가적 사이버 안보 추진체계를 마련해야 한다는 지적이 꾸준히 제기되어 왔음

- 과거 국가사이버안전체계(국가안보실)와 주요기반시설보호체계(국무조정실), 사이버 안보 관련 공공분야(국가정보원)와 민간 분야(과학기술정보통신부) 등으로 이원화된 체계를 유지했는데 이를 통합·개선할 필요성이 꾸준히 제기되었음
  · 국가사이버안전체계는 입법부, 사법부 등 타 기관이나 민간을 직접 규율할 수 없고, 주요기반시설보호체계는 시설지정 범위가 충분하지 못하여 정부 내 협력에 한계가 있었기 때문임
- 국가안보에 있어 사이버 안보의 중요성을 인식하고, 안전한 사이버 공간을 구현·유지하는 노력에 있어
  · 모든 국가기관은 물론, 공공과 민간이 상호 협력하도록 국가적 사이

버 안보 추진체계를 구축할 필요가 있다는 지적이 지속적으로 있어 왔음

- 범국가 차원의 통합 대응체계 확립 차원에서 사이버 공격 발생시 신속하게 정부·기업의 핵심역량을 결집하기 위해 통합 대응조직을 설치, 국가 차원의 합동대응 역량을 강화할 필요성도 제기됨
  · 범국가적 역량을 투입하여 국가 핵심 인프라부터 국민의 디지털 일상까지 보호할 수 있도록 상시 대비태세를 마련할 필요성도 제기됨

○ 이렇게 사이버 안보의 통합 대응체계를 확립하는 과정에서 사이버 안보 전략의 컨트롤타워 역할을 어느 기관이 맡을 것이냐는 논란이 있었으나 2015년 4월부터 국가안보실 내에 사이버안보비서관 직제가 설치되면서 국가안보실로 정리되었음

- 현재 국가 사이버 안보 관련 업무 전반을 조율하고, 중강기 정책방향을 수립·검토하는 최상위 컨트롤타워의 역할을 국가안보실에서 담당하도록 하는 사이버안보 수행체계가 운영 중임 (2022년 대외적으로 발표)
- 컨트롤타워는 사이버 안보의 협력 플랫폼과 허브의 역할을 담당하며, 이를 바탕으로 관계부처·기관 및 기업 간 협업 강화. 주기적으로 현안을 점검

○ 정부는 국가 전 영역에서 사이버안보 정보활동 및 국민안전 보호 대응조치 직무를 수행하고 있는 국가정보원을 사이버위기관리 주관기관으로 정함

- <국가정보원법>에 따라 사이버안보 주무부처인 국가정보원은 국가 전 영역에서 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보를 수집·작성·배포하고,

- 북한·외국 등의 안보침해 행위를 확인·견제·차단하며, 국민안전 보호 대응조치를 수행함

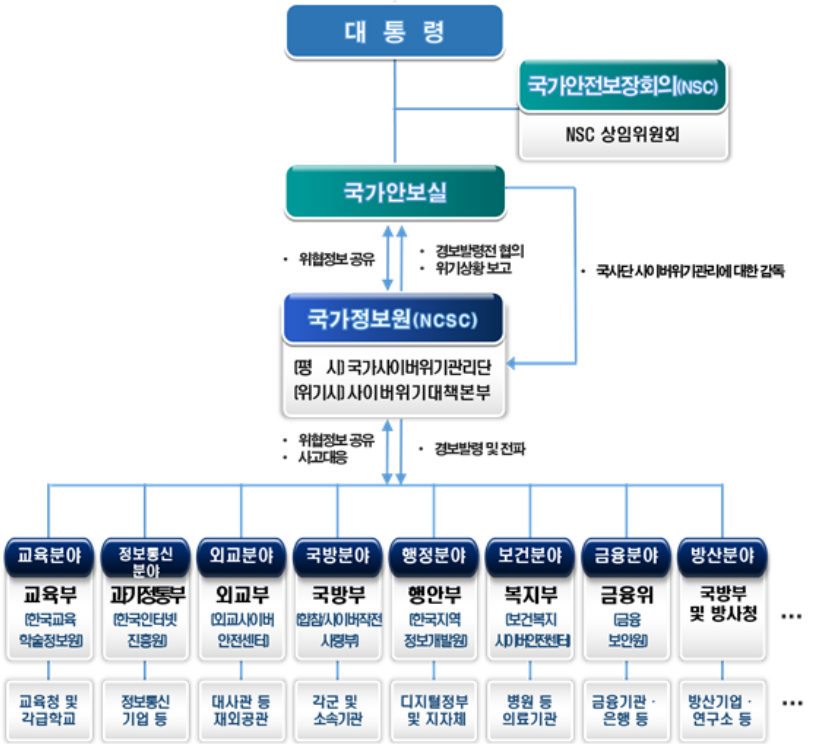
○ 국가안보실과 국가정보원은 지능화·고도화되는 사이버위협에 맞서 일원화된 대응체계를 마련하기 위하여 정부·공공·민간 전문가들이 합동으로 국가 사이버위기 대응활동을 수행하는 국가사이버위기관리단을 국가정보원 국가사이버안보센터 내에 2023년 5월 공식 설치하였음.

- 국가사이버위기관리단은 2023년 3월 개정된 '국가위기관리기본지침'에 따라, 국가정보원과 정부·공공·민간 전문가들이 합동으로 국가 사이버위기 대응활동을 수행
- 국가안보실이 이를 감독하는데 유관부처, 전문기관·기업 등과 실시간 위협정보 공유 및 사이버위기에 대비·대응하고 있음 (18개 기관, 25명이상주; 2024년 상반기 기준)

○ 모든 영역에 걸쳐 발생하는 사이버 안보 위협에 대응하기 위해 국가안보실을 중심으로 정부 각 부처의 각급기관의 역할 및 협력체계를 확립

- 각 부처는 국가정보원법, 전자금융거래법, 정보통신망법, 의료법, 국방정보화법 등 개별 법령에 근거하여 분야별로 사이버 보안 또는 정보보호 활동을 수행 중
- 구체적으로는 △ '국가·공공' 분야는 국가정보원(국가정보원법 등) △ '교육' 분야는 교육부 △ '금융' 분야는 금융위원회(전자금융거래법) △ '정보통신' 분야는 과학기술정보통신부(정보통신망법 등) △ '보건의료' 분야는 보건복지부(의료법) △ '교통' 분야는 국토교통부(자동차관리법) △ '군' 분야는 국방부(국방정보화법)가 각각 보호 활동을 수행하고 있음

〈그림1-1〉 국가 사이버 안보 수행체계 현황



출처: 『2024 국가정보보호백서』 p.10

○ 이러한 컨트롤타워 정립 논의에서 잊지 말아야 할 것은, 사이버 안보에 대한 대응전략은 군사안보와 같은 전통안보를 대하는 전략과는 질적으로 다를 수밖에 없다는 사실임

- 시스템 차원의 불확실성이 커지는 상황에서, 국가 행위자와 같은 어느 한 주체가 나서서 통제하고 자원 동원을 집중하려는 위계조직의 해법은 한계가 있을 수밖에 없음

· 오히려 국가 이외에도 지방자치단체, 기업과 개인 등의 이해당사자

들이 각기 책임지고 자신의 시스템을 보호하는 분산적이지만 자율적인 거버넌스 모델이 효과적일 수 있음

· 더 나아가 주변국이나 해외국의 정부 및 국제기구·단체 등과 적극적인 협력관계를 구축할 필요가 발생함

- 또한 새로운 위협의 창발과 새로운 대응전략에 대한 논의는 오늘날 세계정치에서의 새로운 안보 패러다임의 부상이란 관점에서 이해할 필요가 있음

· 다시 말해, 보이지 않는 버추얼(virtual) 창과도 같은 공격을 막기 위해 필요한 것은, 철벽방어를 목표로 '벽돌집'을 짓는 전통적인 발상이 아니라 나뭇가지 하나하나를 모아서 '그물망'을 짜는 것과 같은 복합적이면서도 유연한 발상임

· 비유컨대, 복합 네트워크 환경에서 발생하는 사이버 위협에 대응하기 위해서는 복합 네트워크 해법을 찾아야 함

【참고】 네트워크 국가와 메타 거버넌스

- 네트워크 국가(network state)란, 대내적으로는 위계적 관료국가, 대외적으로는 영토적 국민국가의 모습을 하는 기존의 근대 국가모델이 글로벌화와 정보화 및 네트워크 시대의 변화하는 환경에 맞추어 자기변화와 구조조정을 해나가는 국가임. 변화하는 국가의 모습은 중앙정부와 지방정부 내의 공조, 국가-민간기업-시민사회의 협업, 지역 및 글로벌 차원에서 진행되는 정부간 협력, 초국적 차원의 연결망 구축 등에서 다양하게 나타남
- '거버넌스의 거버넌스(the governance of governance)'라는 뜻의 메타 거버넌스(meta governance)는 각 분야에서 이루어지는 개별 행위자들의 '거버넌스'를 망라하여 조정하는 네트워크 국가의 '거버넌스'를 의미함. 메타 거버넌스는, 군사안보와 같은 어느 한 영역의 관리에 치중하는 전통안보 분야와는 달리,

여러 분야에 걸쳐서 다양한 유형의 위험들이 창궐하는 신흥안보 분야에 적합한 거버넌스 양식이라고 할 수 있음

2. 사이버 안보의 범부처 공조 체계 정비

○ 정부 각 부처는 그 소관 영역에서 고유한 사이버 안보 역량을 극대화하기 위해 부처별로 권한과 책임을 확립하며 이를 바탕으로 소관 업무를 추진하는 체계를 마련해야 함

- 사이버 안보의 문제는 전통적인 안보와 달리 복잡계의 환경에서 발생하는 신흥안보(emerging security)의 특성을 지니기 때문에 사이버 안보와 관련된 다양한 영역의 개별 역량이 고르게 성장해야 함
- 개별 부처의 업무수행 기반 강화 차원에서 각 부처의 역할과 책임을 유기적으로 연결하여 조화를 이루고 제도화하는 것도 필요함

○ 이러한 소관 부처별 역할 정립을 바탕으로 범정부적 사이버 안보 추진체계를 통해 부처 간의 유기적 협력과 권한의 조정, 업무 조율 등을 수행하는 메타 거버넌스 체계를 구축하는 것이 가능함

- 사이버 위협의 다양한 형태와 잠재력을 고려할 때 특정 부처나 영역의 대응만으로는 한계가 있을 수밖에 없으며, 각 부처의 고유한 대응력을 그물망처럼 엮어내는 전략이 필요
- 각급기관이 수행하는 소관 분야별 사이버 안보 활동에 대한 평가를 시

행하고 후속 보완 조치를 마련하는 체계를 수립할 필요가 있음

- 아울러 사이버 안보 대응력을 실질적으로 뒷받침할 수 있는 사이버 안보 전문 지원체계도 강화할 필요가 있음

○ 개별 법령에 따른 직무 범위를 기준으로 소관하는 분야별 사이버 안보 업무가 제대로 수행될 수 있도록 제도와 기반을 개선

- 사이버 안보 위기에 관한 지침 및 매뉴얼을 제·개정하여 유관 부처·기관들이 취할 조치의 절차와 행동 방침을 구체적으로 마련

3. 사이버 안보 분야 민관협력 체계 정비

○ 사이버 안보 위기에 대응하는 민관협력 체계 정비

- 정부·산업계·학계 등 모든 이해관계자가 협력하여 사이버 안보의 중요성을 인식하고 위협에 공동으로 대응하는 환경 조성
- 공공과 민간의 상호 협력을 기반으로 하는 민관협력의 사이버 안보 대응체계를 구축하고, 지속적이고 효과적인 민관협력을 견인하기 위한 제도적·정책적 기반을 조성
- 아울러 국가 차원의 사이버 안보 위협을 예측하고 위기에 신속 대응할 수 있도록 설치된 민·관 통합 대응조직을 활용하여 사이버 위기관리 능력을 제고

○ 사이버 안보 위협에 대한 원활한 대응을 위해서 무엇보다 중요한 것은

위협정보의 공유임

- 공공과 민간이 함께 사이버 위협정보를 공유·분석하는 등 협력을 활성화하여 사이버 위협을 조기 탐지·전파할 수 있는 체계를 구축하는 것이 필요함
  · 공공·민간의 구분이 없는 사이버 공간에서의 사이버 위협은 대부분 공공분야보다 상대적으로 보안관리가 허술한 민간 분야에서 대부분 발생하고 있는데,
  · 민간 분야는 비용부담이나 기술부족 등으로 인하여 신속한 조치를 하지 않아 피해 규모가 커지고 있는 실정
- 따라서 공공과 민간이 모두 참여하는 사이버 위협정보 공유체계를 마련하고, 정보공유 이전과 이후까지 아우르는 전(全)단계의 민·관 협력 체계를 구축
- 안전기준의 설정 단계에서부터 사이버 안보에 대한 침해를 예방하기 위한 대응체계, 사이버 안전사고 발생시 조치 등 일련의 과정에서 민간의 원활한 협력을 강구하도록 함

○ 공공·민간 영역 간 사이버 위협정보의 공유가 법적 근거의 부재로 이루어지고 있지 못하고 있어 사고 예방에 한계가 발생하고 있음

- 통합 정보 공유체계 구축을 위해 민간이 사이버 위협 정보를 제공할 수 있는 법적 근거를 명확히 하고, 수집·분석된 사이버 위협 정보를 국가적 차원에서 널리 활용하는 기반을 마련해야 함
- 민·관 통합 위협 정보공유체계 구축을 위한 법적 근거와 함께 정보제공에 있어 충분한 개인정보 보호조치를 이행하도록 함으로써 민관협력형 사이버 안보 파트너십을 강화. 정보 제공을 위한 구체적인 절차와

기준을 마련함

· 이를 위해 먼저 정부 내 다양한 위협 정보 수집 기관들이 원활하게 서로 정보를 공유하기 위한 제도와 정책을 구축하고 이를 민간에 확산하는 노력이 우선될 필요도 있음

- 민간의 자율적인 협력을 이끌어 낼 수 있는 기술지원, 보조금 지급 등 다양한 협력 유인정책을 마련할 필요도 있음
- 정부는 사이버 안보 활동에서 수집된 위협 정보를 분석하여 민간에 적시 원활하게 제공함으로써 민간의 사이버 안보 역량 강화에 기여하여야 함

○ 민간 당사자의 협력 활성화를 위한 협력적 플랫폼 구축

- 범국가적 사이버 위기 대응을 위한 민간 역량의 활용을 확대한다는 차원에서 민간 이해당사자 간 협력을 활성화하고 민간 주체의 자율적·능동적 참여를 촉진하는 협력적 플랫폼을 구축
- 유사시 국내 사이버 안보 위협 및 국제적 위기 대응 활동을 지원하는 다양한 분야의 민간 전문인력을 적극적으로 활용하고 이를 확대
- 국가·공공기관 사이버 안보 업무 및 정책 활동에 민간 사이버 전문인력을 활용하기 위해 혁신적 제도와 보상 체계를 마련하여 단계적으로 이행
- 민간과 공공이 함께 참여하는 국가적 차원의 연합 훈련을 추진하고, 국제적인 사이버 방어 훈련을 개최하는 등 세계적 수준의 최첨단 교육훈련 기반을 마련

○ 대국민 인식 제고 및 실천 강화

- 사이버 안보위협에 대응하기 위해서는 사회적 공감대의 조성이 필요
- 국민이 사이버 안보의 중요성과 안전 수칙을 체득할 수 있도록 SNS·대중 매체 등을 활용한 국민 참여형 인식 제고 캠페인을 활성화
- 국민이 사이버 안보 위협에 대한 중요성을 인식하고, 일상에서 사이버 위협에 노출되지 않도록 맞춤형 인식 제고 프로그램 및 콘텐츠를 개발·제공
  · 특히 영세사업자 등 사이버 위협에 취약한 '사각지대'에 대한 지원 필요
- 이러한 사업을 수행하는 정부 기관에 대한 국민적 신뢰가 중요함을 잊지 말아야 할 것임

4. 사이버 안보 외교의 추진체계 정비

○ 사이버 안보 분야의 국제협력에 대응하기 위해 좀 더 효과적인 사이버 안보외교 추진체계를 모색할 필요
- 현재 사이버 안보외교 업무는 유관 부처별로 분산적으로 수행되고 있음
- 사이버 안보외교와 관련하여 외교부, 국정원, 국방부, 과기정통부, 경찰청과 검찰청 등에서 국제협력 활동 진행 중
  · 유엔 정부자문가그룹(GGE)과 개방형워킹그룹(OEWG) 등에서 이루어지는 사이버 안보에 대한 논의는 외교부, 국정원 관련 기관에서 참여, ICANN, ITU/WSIS/IGF 등의 활동에는 과기정통부가 참여, 사이버 범죄 관련 국제협력과 국제회의에는 경찰청과 검찰청이 참여하고

있음

- 그러나 현재 이들 부처의 사이버 안보 관련 국제협력 활동은 상호 조정되지 못하고 다소 분절적으로 진행되고 있다는 지적이 제기됨
- 이러한 상황에서 사이버 안보외교의 추진체계 정비라는 차원에서 유관 부처 간 협력체계 구축의 방안에 대한 고민이 필요할 것임

○ 사이버 안보의 국제협력과 외교의 효과적인 추진을 위해서는 외교 전담부처인 외교부뿐만 아니라 사이버 안보 관련 국제협력 업무에 종사하는 정부 각 유관부처, 그리고 국가안보실 등을 아우르는 추진체계의 정비가 필요할 것임

- 현재 외교부 내 사이버 안보외교 추진체계는 기존의 국제기구나 국제안보 업무로부터 분화되지 못하고, 기존 안보업무의 일부로 다루어지고 있음
- 사이버 안보외교의 효과적인 추진을 지원하기 위해서는 정부 각 부처 또는 외교부 내에서 기존 업무 담당 부서의 재조정 이외에도 새로운 부서나 기관의 신설도 검토할 필요성이 있음
  · 이는 정부 전체 차원에서 실무부처 간의 관계를 설정하는 문제이기도 하고, 또는 사이버 안보외교의 컨트롤타워를 정비하는 차원에서 사이버 안보외교 담당 조직의 신설 또는 재정비 문제이기도 함
  · 최근 외교부 내에서는 '외교전략정보본부'가 출범하여 기대를 모으고 있음
- 이러한 범부처 간 사이버 안보외교 추진체계의 정비 과정에서 사이버 안보의 컨트롤타워 역할을 하는 국가안보실의 역할이 중요할 수밖에 없음

- 국가안보실 내에서 사이버 안보외교의 컨트롤타워 역할을 수행할 세부적인 조직 정비도 필요함
  · 이런 면에서 사이버안보비서관의 사이버 안보외교 업무 총괄 및 그 확장이 기대됨

○ 한편 정부와 국가안보실 내 조직 재정비에 대한 고민과 함께 사이버 안보 분야의 특성을 반영하는 민간(학계) 차원의 1.5트랙 포럼에 대한 연구 및 정책 지원 네트워크의 구축에 대한 고민도 병행되어야 할 것임
- 이러한 과정에서 미중 사이에서 형성될 가능성이 있는 경쟁과 갈등관계 속에서 한국이 추구해야 할 사이버 안보의 국가전략의 방향성을 설정하고 그 내용을 채우는 중견국 외교의 전략과 지식역량을 갖추는 것이 필요함
- 이를 위해서 외교 역량의 배양이 필요하며 실무 차원의 복합적인 외교 마인드의 모색과 함께 정책대안에 대해서 고민하고 연구하는 학계의 노력이 뒷받침되어야 함.

5. 사이버 안보 분야 법제도 정비

○ 국가 차원의 사이버 안보 대응체계를 정립하고, 실질적이고 구체적인 사이버 안보 활동의 법제도 기반을 마련할 필요가 있다는 요구가 증대
- 현재 한국의 국가적 사이버 공격 대응 활동은 각 부처별 소관 개별 법령에 따라 제각각 분리, 독립 대응하고 있어 국가 사이버 안보 위협 상

황 발생 시 범정부 차원의 종합적 대응에 한계가 있다는 지적

- 정보통신망, 전자정부, 국가안보, 국방, 금융 등 각 부처가 경쟁적·수평적·산발적으로 법제 및 정책을 추진하고 있어, 사이버 안보 관련 법체계, 행정권한 등에 있어 혼선을 초래하고 민·관간의 협력체계가 취약한 실정임

  ※ △ '국가·공공' 분야는 국가정보원법 등 △ '금융' 분야는 전자금융거래법 △ '정보통신' 분야는 정보통신망법 등 △ '보건의료' 분야는 의료법 △ '교통' 분야는 자동차관리법 △ '군' 분야는 국방정보화법 등

- 공공과 민간의 연계 부족, 수평·분산적 대응체계의 한계를 극복하기 위해 사이버 안보 법제도 확립 필요

○ 범정부적 사이버 안보 추진체계, 공공과 민간의 소통과 협력, 개인정보 보호, 국제협력 등 사이버 안보 관련 법적 기반 강화를 위한 법제도 개선을 추진

- 새로운 사이버 안보 법제는 민간과 공공 간의 유기적 협력을 이끌어 내고, 각 부처 간 역량을 극대화하면서도 범정부적 조정기능을 내실화하도록 함
- 법제도 개선은 사이버 안보가 정부, 기업, 개인 등 사이버 공간의 모든 주체에게 중요한 가치임을 인식하는 데에서 출발하여야 하며,
  · 공공과 민간을 종합적으로 대응하면서 신뢰에 기반을 둔 민관협력을 추진할 수 있도록 개인정보 보호 등 정보인권도 소홀하여서는 아니 됨
- 이러한 법제도 개선을 통해 국내 사이버 안보 대응력 강화는 물론 원활한 대외 국제협력을 위한 입법적 전기를 마련해야 함
- 사이버 안보 법제 개선의 방식은 독자적인 신법의 제정, 기존 법령의

개정을 비롯하여 현행 법제의 운용을 정상화하는 등 다양한 방식이 가능

○ 돌이켜 보면, 사이버 안보 관련 법제정을 둘러싼 서로 다른 의견이 제기되어 왔음
- 핵심 쟁점은 국가 사이버안보 거버넌스에 있어서 국정원이 어떤 역할을 하느냐에 대한 것이었음
- 그러나 이와 관련해서는 국회가 2020.12월 국가정보원법 전부 개정을 통해 국정원의 사이버안보 직무 범위를 명시함으로써 그동안의 논쟁에 대해 입법적으로 종지부를 찍었음

○ 법제도의 개선은 사이버 안보와 개인정보보호의 조화로운 발전을 담은 내용을 통해 사법 통제 등 법치주의 원칙에 기반을 두어 국가와 시민사회 모두의 공감대와 합의를 이끌어 내도록 해야 할 것임
- 사이버 안보는 정부, 기업, 개인 등 사이버 공간의 모든 주체에게 중요한 가치임을 인식하고, 사이버 안보 법제 개선은 국가와 시민사회 모두의 공감대와 합의를 기반으로 추진해야 함
- 시민사회가 사이버 안보를 위한 대응과정에서 개인정보보호 등 정보인권이 소홀하게 취급되지 않을 것이라는 신뢰를 가질 수 있도록 충분한 개인정보보호 장치를 마련할 필요
- 사이버 안보 대응을 위한 개인정보의 합법적 이용 근거를 명확히 하고, 개인정보 비식별화 조치기준 등 안전하면서도 능동적인 정보 수집·분석을 위한 구체적인 방안을 마련하도록 관련 절차를 마련

○ 새로운 법제는 각 정부 부처의 역량을 극대화할 수 있도록 권한과 책임

을 강화하도록 하면서도 기존 법제와의 충돌을 방지하여 영역별 개별 법제와의 상호작동성을 제고해야 함

- 현행 법제는 범정부적인 조정 기능의 취약성과 맞물려 사이버 안보 대응 능력을 저하시키는 주요 원인이 되고 있는 바,
  · 법제 개선을 통해 각 부처 소관 법률간 규율대상의 중복 내지 불분명, 부처 간 권한 혼선 등을 해소할 필요
- 사이버 안보 대응력 제고를 위한 개별 법제 정비를 지속적으로 추진하고, 각 부처의 집행력 강화와 함께 권한의 오·남용을 방지하기 위한 적절한 통제 장치를 마련할 필요

제2장

사이버 정보공유 및 대응역량 강화

김 소 정 | 국가안보전략연구원 책임연구위원, CSIS 객원연구원

1. 사이버 정보 수집·분석 및 공유 기반 강화
2. 사이버공격 대응을 위한 기준 고도화 방안
3. 공세적 방어 역량 확보 사례와 방안
4. 가짜뉴스 대응, 선거개입 등 영향력 공작 대응방안
5. AI 도입에 따른 사회적 대응역량 강화

제2장

사이버 정보공유 및 대응역량 강화

김 소 정 | 국가안보전략연구원 책임연구위원, CSIS 객원연구원

배경과 구성

- 국가 사이버 안보 전략은 리질리언시(resiliency) 강화 및 확산, 기관간 정보 수집·분석 및 공유 강화, 공세적 방어 역량 확보, 영향력 개입 대응 등을 주요 과제로 설정함
- 국가 차원의 사이버 리질리언시 강화 및 확산, 정보 수집·분석 및 공유 강화, 공세적 방어 역량 확보, 사고대응 기준 고도화, 가짜뉴스 등 영향력 공작 대응을 위한 정책 현황을 분석하고, 향후 정책 발전 방안 제시할 필요가 있음
- 제2장의 구성은 아래와 같이 다섯 가지 항목을 중심으로 함
  1. 사이버 정보 수집·분석 및 공유 기반 강화
  2. 사이버공격 대응을 위한 기준 고도화 방안
  3. 공세적 방어 역량 확보 사례와 방안
  4. 가짜뉴스 대응, 선거개입 등 영향력 공작 대응방안
  5. AI 도입에 따른 사회적 대응역량 강화

1. 사이버 정보 수집·분석 및 공유 기반 강화

○ NCSC를 중심으로 위협정보공유체계 운영중, 특히 NCSC의 NCTI는 방산업체 등 주요 기반시설 관리기관을 포함한 특정 업종에도 지속적 정보공유를 통해 사회전반적 사이버안보 수준 향상, 위협대응 공조 강화 추진 중

- 대외적으로는 기관별 협력채널을 통해 위협정보 공유 중, 특히 협력을 문서화한 미·영 등 경우 공식적 정보공유 채널을 확보했을 것으로 추정
- UN 사이버안보 개방형 워킹그룹(Open-Ended Working Group, OEWG)은 국가별 Point of Contact(PoC)를 확보하고, Directory 구성을 추진 중 (2024년 5월 현재 91개국 참여 중)

【UN OEWG PoC Directory 구축 계획】

· UN은 PoC 구축을 통해 국가별 책임있는 ICT 이용이 가능한 환경을 구축하고, 사이버공간에서 오해로 인한 갈등을 경감시키고자 노력해 옴

· 지정학적 경쟁이 강해지고, 상호간 신뢰 구축 및 재구축이 필요한 시점에 Directory구축은 ICT 사고 발생시 직접 대응과 예방을 지원함으로써, 국제적 평화와 안보 위험예방 노력을 강화할 것으로 기대됨

○ OEWG의 Global PoC Directory 구축에 적극 참여

- OEWG가 추진하는 다층적 Global PoC Directory 구축에 적극적으로 참여하여 글로벌 사이버안보 강화에 기여하여야 함
- 다만, 공유되는 정보에 대한 보안성 및 기밀성 유지 방안, 접근제어, 보관 및 처리 후 폐기 등 정보 생명주기 전체 보안 고려 필요
- 외교, 정책, 기술 등 다층적 PoC 간 정보공유 활동 중복, 혼란 초래 등 가능성 있으므로, 국내에서 수신된 공유정보의 종합판단 체계 마련 필요

- Directory는 외교, 정보, 법집행 등 영역별 PoC를 지정할 수 있도록 권고하고 있어, 실제 사고 발생시 오히려 혼선이 가중될 수 있으므로 책임과 권한, 명확한 의사결정체계를 구체화해야 함
  - 기존 정보공유 채널과의 중복문제가 발생할 가능성이 있으며, 국가 CERT로 지정된 CERT간 협력을 기본으로, 기존 FIRST 협력 체계 조정 필요
  - 예를 들어, FIRST에는 Kr-CERT가 대표로, 국가 CERT는 Kn- CERT로 지정되어 있음. 이에 대한 조정 및 각 CERT간역할 및 체계 조정 등 고려
  - 현재도 단일 외국 기관에 한국의 다수 부처가 협력 요청을 하거나 MOU 추진 등을 요구해 상대측 기관에서 혼란스러워하는 경우가 종종 발생함
  - 또한 수집 및 공유된 정보를 바탕으로 일원화된 정책결정이 가능하도록 부처별 협력체계들과 중복되지 않는지, 필요한 경우 상호 간 조정 진행 가능

- 서방의 격자형 안보구조 재편에 따른 동맹국 및 우방국들과의 정보공유 채널 확대, 혹은 기존 정보공유 채널에 편입 방안 고려
  - 기술적 정보공유는 활성화되어 있는 반면, 안보적 측면의 정보공유 측면에서 기존 국가간 협력체계 내에서 정보공유 활성화 방안 검토 필요
  - 예를 들어, Five Eyes 참여(혹은 확대된 Five Eyes에 사이버 위협정보를 중심으로한 별도 정보공유 체계 신설), AUKUS Pillar 2에 한국도 참여, NATO CCDCOE 중심의 사이버위협정보 공유 강화 등 고려 가능

- 정책 및 외교적 측면의 정보공유 시 공유되는 정보의 체계, 형식, 중요도, 보안 등 고려 선행 필요
  - 기존 외교, 정책 채널에서 사이버위협정보 공유는 기술 채널의 사이버

위협정보와 공유되는 정보의 형식, 내용 등에 차이 발생 가능

- 참여자들 간 이에 대한 조정 및 절차적 합리성 보장 방안 마련 필요
- 기존 정보공유 채널과의 중복문제 발생 가능성이 크며, 국가 CERT로 지정된 CERT간 협력을 기본으로, 기존 FIRST 협력체계 조정 고려 필요
  · 2023년 하반기 국가 사이버안보 거버넌스 변경에 따른 CERT간 협력 채널, 정보공유채널 등에 대한 재조정 요소 식별 및 조치 시행 필요
  · 사이버공간 갈등시 대응 효율화 측면에서, 현재의 분산된 체계에 대한 정비가 필요한데, 예를 들어, FIRST에는 Kr-CERT가 대표로, 국가 CERT는 Kn-CERT로 지정되어 있음, 이에 대한 조정 및 각 CERT간 역할 및 체계 조정 등 고려

2. 사이버공격 대응을 위한 기준 고도화 방안

○ 고도화되고 점증하는 사이버공격에 대응하기 위해 우리나라는 단독 혹은 우방국과 협력하여 사이버공격에 대한 제재 부과, 합동보안권고문 발표 등 지속

- 그러나, 공개된 사이버공격 대응을 위한 기준 및 정책 부재
- 최근 공개된 국가 사이버안보 전략 기본계획에는 “최신 공격기술, 국내외첩보를 포괄한 범국가 위협정보 DB 구축과 유관기관 합동 평가를 통해 공격주체 판단의 객관성 및 정확성 제고”를 추진할 예정이라고 밝힘
- 또한 “배후 지목을 위한 절차 및 기준 수립 등 국제공조 대응을 위한 기반 구축”도 추진 예정

○ 사이버 위협환경 변화에 따른 우리의 인식, 판단 및 대응 정책과 근거 공개 개시방안 마련[1)]

- 구체적이진 않으나, 심각한 위협으로 국가차원의 대응이 필요하다고 생각되는 수준에 대한 개괄적 정책과 근거 개시 필요
- 중대 사이버사고 대응 시 연방기관 간 역할을 규정한 문서 개발 및 이에 따라 사이버 사고 발생 시 각 기관은 주요 침해사고로 판단 또는 관련 내용 보고 절차 등 마련
- 국가안보, 경제 등에 영향을 미치는 사이버 사고 발생 시 연방정부에서 공통된 시각으로 사이버 사고의 심각도를 평가하도록 심각한 정도를 단계별로 정의
- 심각한 사이버 침해사고에 대한 정의 마련 및 이에 따른 대내적 처리 절차 준수 요구
- 국가 차원에서 사이버 사고 위험을 평가하여 점수화하고, 평점에 따라 공공 자원 배분 우선순위 결정을 위해 국가 사이버 사고 평점 체계 개발 등

○ 사이버 사고 발생시 △사고의 심각성 △사고 대응의 시급성 △대응활동 조율에 필요한 직급 수준 △대응활동에 필요한 투자에 대해 관련 연방기관들의 공통된 인식에 기반한 대응을 위하여 제시된 분류체계 마련

- 필요시, 기준 및 대응을 위한 연구개발 등 병행

1) 김소정, "미국의 사이버공격 대응정책과 한국에의 시사점 : 솔라윈즈 해킹 대응사례를 중심으로", 국가안보전략연구원 INSS 연구보고서 2022-04, 2022년

○ 공개하는 정책과, 이에 따른 국가 대응의 합법성과 근거 확보 필요

- 국가차원의 대응이 제재 등에 이르는 경우, 대내적 근거 마련 필요
- 적대적 외국이 관련된 사이버 위협 및 그 심각성, 귀속 판단을 위해 전 부처의 역량을 집중하고, 이를 바탕으로 각 부처 및 군의 직무 영역에서 가용한 대응 행동을 취하도록 절차 마련
- 이를 지원할 수 있는 제도적, 절차적 정당성 확보 방안 마련 필요

○ 또한 국가 혹은 국가후원 단체의 악의적 행위에 대한 책임을 부과하기 위해서는 명확한 공격자 식별이 중요하며, 이에 대한 기준 마련 필요

【미국 사례】

- 사고 인지 단계에서 단순 사이버사고와 중대한 사이버사고에 대한 정의, 사이버 사고에 대한 기관별 책임 수행체계 명시한 대통령 명령 공개
- 국가 사이버 사고 평점 체계를 개발, 사이버 사고 위험을 평가하고 정보 수집, 사이버 사고 심각도 단계 개발 및 적용
- 악의적 사이버 활동을 국가비상사태로 지정하고 제재를 부과할 수 있도록 근거법을 마련, 특히 북한 정부 등의 재산과 거래를 포괄적 금지 및 제재 명시

	정의	기존 법제·정책상 유사 개념
사이버 사고	컴퓨터 네트워크 상에서 혹은 이를 통해 일어나는 사건으로, 컴퓨터, 정보 또는 통신 시스템이나 네트워크, 컴퓨터나 정보 시스템에 의해 통제되는 물리적 또는 가상 인프라, 또는 이에 저장된 정보의 무결성, 비밀성, 가용성을 실제로나 임박하게 위태롭게 하는 것으로, 정보 시스템, 시스템 보안 절차, 내부적 컨트롤, 실행상 취약점 등을 포함	사고(incident) (A) 정보나 정보시스템의 무결성, 비밀성, 가용성을 실제로나 임박하게 위태롭게 하는 현상; 또는 (B) 법률, 보안정책, 보안절차, 또는 용인되는 이용 정책의 위반이나 위반의 임박한 위협 현상[2014 FISMA]

	정의	기존 법제·정책상 유사 개념
중대한 사이버 사고	사이버 사고 중 (또는 총체적으로 그러할 수 있는 연관된 사이버 사고들의 그룹) 미국의 국가안보 이익, 대외관계, 경제나 미국인의 대중적 신뢰, 시민적 자유, 또는 공중의 보건과 안전에 대하여 드러나는 피해를 야기할 수 있는 것.	주요사고(major incident) [2015 OMB 가이드라인]

3. 공세적 방어 역량 확보 사례와 방안

○ 미국은 2018년 국방 사이버전략부터 지속적 개입(Persistent Engagement)과 전진 방어(Defend Forward) 전략을 사이버전 수행 개념으로 명시, 이에 기반한 작전(Hunt Forward)을 수행함

- (개념) 심각한 사이버 공격의 위험을 줄이고, 무력 충돌의 임계치 이하 수준의 저강도 사이버 행위(분쟁)들에 대응하기 위한 접근법
- 러시아-우크라이나 전에서 우크라이나를 지원하거나 실제 우크라이나와 작전 시행 등 사례 다수 언급
- 사이버공간을 통한 미국 공격 시 비용과 이점 계산 방식 변경을 유도하는 적극적 공세적 방어역량을 확보하는 지속적 개입과 전진 방어 활동에 무게가 실리면서, 공세적 활동의 단독 및 다국간 작전인 hunt forward 지속 수행 중

○ 미국은 2023년 국가 사이버안보 전략을 공개, 국가주요기반시설 보호를

강조하고 있음. 사이버안보에서의 정부의 역할을 강조하고 종합적 접근을 시도하는 한편, 양자 및 AI 분야 등 신기술 발전과 국가안보, 보안생태계 구축 필요성 제기

- 또한 민간부문과의 협력을 강화하고 국제무대에서의 악의적 행위자 대응을 위한 자발적 노력 강화와 규범적 역량 강화의 측면을 동시에 추진 중
- 무력공격 이하 수준의 저강도 분쟁 유발시 적이 감수해야 할 비용을 사전에 미리 관찰하고 추적하여
- 전략적 환경을 재구축하고 악의적 행위에 드는 비용을 막대하게 함으로써 현재 진행되고 있는 악의적인 사이버 캠페인을 저지하고, 미래의 캠페인 발생을 억지하며 우호적인 국제 행위규범 재구성하는 것을 목표로 함

○ 공세적 사이버 방어활동 역량 확보를 2024년 전략의 주요 특징으로 언급

- 공세적 대응, 공세적 사이버 방어, 선제적 방어, 억지력 확보 등 용어가 전략에서 다양하게 언급됨

○ 국가 사이버안보 전략 기본계획은 “국제 및 국가배후 해킹조직 등 위협 행위자를 식별하고 해킹 거점과 인프라 및 활동을 추적하는 기술 개발” 명시

- 또한 “사이버보안 권고문 발표에 따른 위협 억지 효과 극대화를 위해 다수 자유진영 국가 참여하여 위협 행위자, 실태 폭로 등 국제적 연대 강화” 추진 명시
- 국가안보 위해활동에 대한 공세적 대응 강화, 위협정보 수집·분석 기반 강화, 사이버범죄에 대한 예방·대응역량 제고

○ 용어 및 개념 구체화 필요

- 공세적 대응과 공세적 방어, 선제적 방어, 억지는 이론적으로 명확한 개념정의 기반해 전략서에 언급되는 것이, 국가 정책 추진 방향을 명확히 해줄 수 있음
- 적극적 방어와 발생한 피해에 대한 적극 대응은 공격국/단체에 대한 공격행위를 의미하지 않음에도 불구하고, 공세적 방어라는 단어를 공격의 의미로 적극적 해석하는 경우, 불필요한 갈등 조장 및 오해 발생 가능성 있음

○ 지속적 개입(Persistent Engagement)과 선제적 방어(Defend Forward) 전략 개념의 이해 및 군 적용 현황, 군 작전 시행 현황 등을 분석할 필요

- 전진방어 개념 적용시 고려해야 할 주권, 대응조치, 개입, 식별 등과의 상관관계 분석
- 전진 방어 개념의 국내 적용 가능성 모색, 정보 및 군 차원 적용 가능성 연구
- 정보 및 군 차원 사이버 분야 실무협력을 위한 전략개념 분석 및 국내 적용을 위한 고려사항 식별
- 전진 방어 개념에 기반한 국외협력 및 전략 개발시 참고

○ 기술적 활동 강화의 제도적 근거 고려 필요

- 공격 근원지 식별, 추적 대응 시스템 고도화 등의 대상이 국내 네트워크를 벗어나는 경우에 대한 고려 필요
- 안보 목적의 수사 시 근거가 될 수 있는 적법절차 구체화 및 현행화 필요

4. 가짜뉴스 대응, 선거개입 등 영향력 공작 대응방안

○ 국가 사이버안보 전략은 영향력 공작, 허위정보 유포 및 확산, 가짜뉴스, 여론 조작 등에 단호히 대처하고, 인식을 제고할 것을 설명

- 최근 공개된 국가 사이버안보 기본계획은 공세적 사이버 방어활동 강화를 위해 사이버공간상 영향력 공작 대응 강화를 주요 계획으로 선정
  · 범부처 합동 대응방안 구축, 해외발 허위조작정보 및 영향력공작에 대한 효과적 대응체계 마련을 위한 법제 정비, 허위정보 탐지·대응 체계 수단 확보, 불법정보 차단 업무 역량 제고 및 유관기관 협력 강화 등 추진 예정
- 최근 미국 국무부와 한국 외교부는 허위조작정보 및 영향력 공격 대응 협력을 위한 양해각서 체결
  · 한국 정보기관 및 외교부는 관련 대응체계 구축을 위한 조직개편 추진 중

○ 영향력 공작, 허위정보 유포 및 확산, 가짜뉴스 생산 및 유포, 여론조작 등에 대해 지속적으로 관심을 가지고 체크할 수 있는 연구기관, NGO 등 활동 장려 필요

- 정부부처 중심의 정보 제공 및 대응은 정치적으로 악용될 가능성이 높으며, 신뢰도 확보에 어려울 수 있음
- 정보공개로 확보된 데이터는 공격 주체별 관리, 주요 타겟 분야 대응력 향상 등 추가적 정책 활용 가능성도 높음
- 다양한 소스의 자료를 통해 객관성과 신뢰성을 확보하고, 투명성을 담보할 수 있는 체계가 관련 대응의 시초가 되어야 함

○ AI 등 신기술 활용 대응을 위한 기술적 측면의 연구지원 강화 필요

- 미국은 데이터 확보, 신기술 적용 등을 포괄한 다층적 대응 방안을 고려 중이며, 다양한 연구기관 및 NGO 등과 협력 체계 구축
- 유연하고 적응력 있는 전략을 마련, 지속적인 연구개발(R&D) 투자와 함께, 보안 전문가 및 정책 전문가들이 협력하여 새로운 위협에 대한 대안 모색
- 분석이 가능한 실제 데이터를 지속적으로 생산하고, 2차 분석이 가능하도록 지원해야 다각도의 유연성 있는 분석과 전략 수립 지원 가능

○ 하이브리드 위협 대응을 위한 국제협력 강화 필요

· 다국적 협력의 틀 안에서 정보와 자원을 공유하는 것이 필수

· 정보공유 채널을 통해 하이브리드 위협이 탐지되는 즉시 적절한 대응이 가능하며, 다른 국가들이 해당 위협을 사전에 인지하고 대비

· 정보기관, 보안업체, 국제기구 간의 네트워크를 통해 구축될 수 있으며, 구체적인 정책 협의와 공동 훈련을 통해 강화 필요

○ 통합적으로 관리할 수 있는 거버넌스 체계 구축 필요

- 군사, 외교, 경제, 정보 분야 전문가들이 참여하는 통합적 대응 기구를 구성하여, 각 분야의 협력 조정
- 허위조작정보를 통한 사회혼란 발생 시 이를 탐지 및 대응하는 제도적 기반을 마련하고, 무·유형 위협에 따른 위험과 피해 산출방안, 국가 차원의 대응과 국제협력이 가능한 위험 수준에 대한 객관화 및 계량화 등 정책 결정 기초자료 확보와 생산가능한 환경 조성 필요
- 이를 지원하고 다양한 부처 간 협력을 조율할 수 있도록 전문 연구기관의 플랫폼으로써의 역할도 강화

○ 법적 규제와 제도 개선 필요

- 사이버 공격이나 정보전에 대한 처벌을 강화하고, 특히 비국가 행위자나 테러리스트들이 이러한 위협을 조장하는 경우 국제법적 차원의 대응 방안 강구
- 국제 형사 재판소나 유엔 등을 통해 제재 및 법적 대응을 강화할 방안을 모색하고 전문가를 양성

○ 영향력 공작의 주요 목표는 사회의 불안정성을 조장, 사회적 인식 및 회복력 강화방안 마련 시급

- 교육적 캠페인, 미디어 리터러시 향상 프로그램, 허위 정보에 대한 교육 등의 시행을 통한 회복력 강화 도모
- 이러한 프로그램을 통해 일반 국민이 허위 정보를 구별하고, 정보전에 대한 민감성을 가지도록 계도

※ 고려사항 : 미국은 국무부, 국방부, 정보기관 등이 모두 관련 업무추진체계를 갖추고 있어, 실제 운영상 기관별 역할과 임무, 조정통제 현황 등 추가 연구 필요(공개 자료 제한)

5. AI 도입에 따른 사회적 대응역량 강화

○ 각국은 AI를 국방 현대화와 군사적 우위의 핵심요소로 간주, REAIM, AI 정상회의 등을 통해 AI의 기술개발에 따른 사회적 영향력 확대, 정부기관 접목 등 방안 모색 중

- 각국은 책임있는 AI의 군사적 이용에 관한 국가 프레임워크, 전략 및 원칙을 공개하고, 관련 이니셔티브들을 지속적으로 추진.
- 특히 AI의 급속한 도입으로 야기될 수 있는 사회적 비용, 영향, 기회와 도전, 인간과 기계의 협업 사례와 결과 분석, 긍정적 해결을 위한 방법론 및 솔루션 제시를 전문적 연구 주제로 제시

○ 미국의 AI 행정명령은 AI의 사이버보안적 활용뿐만 아니라, R&D, 표준화, 공통평가기준 및 상호인정 등 획득정책, 인권보호, 이민정책 등 다 방면을 고려하여 정부 전체적 접근방식 취하고 있음
- 국방 AI 전략을 통해 의사결정 속도와 정밀도를 향상시키고, 전투 준비 태세를 강화하며, 국제 협력을 통해 윤리적 규범 증진

○ 국가 사이버안보 전략과 기본계획은 AI의 기술개발 측면에 제한적 접근 중, 특히 사이버보안 측면에서 AI 기술을 공격, 방어 양 측면에서 활용하는 방안 고려 중
- 이 외 무기체계에 포함시킨 기술개발 연구, 혹은 기존 무기의 역량을 강화시킬 수 있는 측면의 제한적 AI 활용을 논의 중임

○ 국가적 이익 달성에 부합하는 정책지향점을 수립하고, 범정부 AI 적용과 활용에 관한 미래 시나리오의 개발과 전략 및 로드맵 수립 필요

○ 정부기관용 혹은 국민 대상 정부시스템의 AI 기술 활용 방안 연구
- 사이버보안 측면, 무기개발 측면 외에도 AI를 활용한 대국민 서비스 개발 방안 고민 필요

- 시장 및 상업적 측면, 규제 측면, 이용자 보호 측면, 외교·규범적 측면 모두가 고려되어야 함. 표준화, 기술개발, 디지털 민주주의, 안보 및 보안, 군사적 이용 등 사회 전반에 대한 AI 활용과 부작용 대비 필요

【융합적 정책지향성 설립을 위한 질문 예시】

- 우리의 기술력은 어느 수준인가? 강점과 약점은 어디인가?
- AI 발달이 사회에 가져올 변화는 어떤 것인가? 예를 들어 초고령사회로 들어가고 있는 우리나라는 AI를 긍정적으로 사용할 수 있는 기회가 있는가?
- AI 기술발달로 예상되는 다른 부정적 영향은 무엇인가? 긍정적 영향은 무엇인가? 단편적이지 않게 사회전반에 대한 적용과 고려를 해보았는가?
- 우리가 추구하는 AI의 기술발달상은 어떤 모습인가? 그 과정에서, 또 AI 기술 생태계에서 한국이 갖는 위치는 어디인가?
- 우리 AI R&D 계획 및 AI 안전성 및 보안성 보장 대책은 무엇인가?
- AI 안전연구소의 운영 목적과 추진 방향은 무엇인가? 등

○ AI 규범 논의 참여 활성화

- 사이버안보 규범의 사례에서와 같이, 단시일 내 AI의 군사적 사용에 대한 합의를 이끌어 내기에는 한계가 있을 것으로 판단됨. 그러나 이를 저지하거나 감시해 사후적으로 대응하는 것은 무용하다고까지 볼 수 있음
- 사이버안보적 측면보다 훨씬 더 직접적으로 개인의 생명에 영향을 줄 수 있으므로, 필요성과 시급성은 굉장히 높은 이슈임
- 그러나, 어느 국가도 기술개발시 이를 고려한 개발을 주장하거나, 또는 이를 검증 및 입증할 수 있는 입장이 아니어서, 각국의 자발적 규범 수용 의지에 기대할 수밖에 없다는 한계는 명확함

- 기술적 측면에서 AI의 핵심 알고리즘 개발 역량과 기술력의 국가별 편차가 큰 상황에서 기술력을 보유하고 있지 않은 나라는 생산되는 기술을 그냥 사용할 수밖에 없는 처지임
- 규범적 접근 외에 기술 비보유국의 의지를 반영할 수 있는 기회는 사실상 없다고 할 수 있으며 이러한 상황에서 규범적 접근이 거의 유일무이한 방법임

○ 포괄적 국가 AI 전략 수립 필요

- 데이터 관리, AI기술개발, 인프라 구축 등 다양한 측면을 포함한 기본 전략이 필요
- AI 인지 개발에 투자하고, 민관 협력을 강화
- 데이터 표준화, 상호운용성 확보, 독립적 국방 데이터 플랫폼 구축 등 데이터 생태계 강화를 통해 AI활용도 극대화 모색

○ 정책 고려 사항

- 정책지향성, 전문인력의 부족, 학제간 소통 및 문제의식 공유 부재, 정책결정 지원 가능한 자료 생산의 한계, 국가 R&D와의 정합성, 지속적 실행력 확보 등 전 국가차원의 노력에 AI 측면 고려 필수
- REAIM 및 AI 정상회의 등을 기반으로 한국 내 전사회적인 접근이 가능할 수 있는 체계를 마련하고 이를 지속, 논의 주제도 군사적 사용 외 민간 사용, 기술개발의 정책적 함의, 표준, 윤리 및 인권적 측면 등까지 포괄 고려 필요

제3장

사이버 범죄 및 테러의 예방·대응 역량 제고

윤 민 우 | 가천대학교 경찰행정학과 교수

1. 사이버 범죄-테러 통합정보센터 구축
2. 사이버 범죄-테러 대응을 위한 수사 전문성 강화
3. 사이버 범죄-테러 피해에 대한 신속 지원체계 강구
4. 사이버 범죄-테러 기관 간 공조 강화
5. 사이버 범죄-테러 대응 국제협약 가입

제3장

사이버 범죄 및 테러의 예방·대응 역량 제고

윤 민 우 | 가천대학교 경찰행정학과 교수

배경과 구성

- 사이버 범죄-테러-에스피오나지는 은밀성, 익명성, 무경계성, 시간적-공간적 동일성이 지배하는 비물리적 공간인 사이버 공간에서 벌어지는 위협임
- 따라서 이와 같은 회색지대에서 벌어지는 위협의 특성은 국가의 주권과 범죄-테러-에스피오나지의 물리적, 시간적 제한, 상대적으로 높은 식별성 등을 기반으로 하는 오프라인의 위협과는 질적으로 다름
- 이 때문에 물리적 공간에서의 대응을 염두에 두고 마련된 기존 형사사법과 정보대응 시스템은 제대로 작동하기 어려움
- 결국 사이버 공간의 회색지대적인 특성을 반영한 국가의 정보-수사 시스템을 법제도적으로 마련할 필요가 있으며, 이 같은 특성이 정책 수행에도 반영되어야 함
- 기존 사이버 위협 예방 및 대응 체계의 한계를 인식하고, 이를 보완한 보다 혁신적이고, 효과적인 사이버 위협 대응 정보수사 시스템을 구축할 필요 있음

- 제3장의 구성은 아래와 같이 다섯 가지 항목을 중심으로 함

  1. 사이버 범죄-테러 통합정보센터 구축
  2. 사이버 범죄-테러 대응을 위한 수사 전문성 강화
  3. 사이버 범죄-테러 피해에 대한 신속 지원체계 강구
  4. 사이버 범죄-테러 기관 간 공조 강화
  5. 사이버 범죄-테러 대응 국제협약 가입

○ 본격적인 논의에 앞서 사이버 범죄 및 테러의 진화와 그에 대한 예방 및 대응의 해외 동향을 알아볼 필요가 있음

○ 사이버 범죄 및 테러는 점점 사이버 공간에서의 해킹, 랜섬웨어 공격 등 기술공격위협과 사이버 공간을 활용한 사이버 불링, 온라인 성착취물, 극단주의 유포, 영향공작 등 사이버 정보-심리 공격위협으로 다변화, 복잡화되고 있음

- 사이버 기술공격위협과 사이버 정보심리공격위협 역시 '핵앤릭(hack-n-leak)' 사례에서 보듯, 통합-연계되어 가는 추세임
- 미국이 주도하는 자유민주주의 동맹의 열린 글로벌 인터넷과 정보의 자유로운 소통 진영과 중국-러시아 주도의 국가 통제와 국가주권을 강조하는 권위주의 진영 간의 디지털-사이버 공간 분리와 진영 간 단절이 점점 더 강화되어가는 추이임
- 이 같은 디지털 진영 간의 분리를 의미하는 디지털 지정학적 대치가 강화됨에 따라 사이버 범죄-테러에 대한 각 진영의 대응은 서로 분절적으로 되어갈 개연성이 커지고 있음
- 사이버 범죄-테러를 국가 행위자가 배후에서 민간 프록시(proxy)로 이

용하는 에스피오나지와 사이버 전쟁으로 연계-통합되어 감에 따라 사이버 범죄-테러가 점점 더 국가안보의 문제로 그 의미와 비중이 진화함

○ 미국 등 자유민주주의 선도국가들은 점점 더 사이버 범죄-테러 대응에 있어 공세적 방어, 국가 주도의 해킹과 보복공격, 비밀수사와 공격적 정보수집 등으로 점점 대응을 적극적으로 강화하고 있음[1)]

- 이 같은 추이에 따라 보다 더 적극적이고 공세적인 입법이 마련되고 있음
- 사이버 범죄-안보의 문제를 디지털과 AI, 반도체 공급망, 양자컴퓨팅, IoT, 3D 프린팅 등 관련 신기술과 소재, 부품, 장비 등의 문제와 점점 더 통합적으로 인식하고 대응
- 사이버 범죄-테러에 대한 대응을 '다중이해당사자주의(multistakeholderism)'에 따라 점점 더 정부-민간-군이 함께 통합 대응하는 방향으로 진화하고 있음

1) Cybersecurity Laws and Regulations USA 2024 https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa; Global Cybersecurity Outlook 2024: Insight Report January 2024 https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf?_gl=1*mbbjxn*_up*MQ..&gclid=Cj0KCQjwiYOxBhC5ARIsAIvdH53fHnKk9J07uvKITmiW0Fvalo7yuZy8_sqsZhFkEp0aNWNhzHe0soIaAiAkEALw_wcB; Guidelines to Fight Cybercrimes and Protect Victims, the report of Milan Public Prosecutor's Office, April 2015 https://rm.coe.int/16803060a7; The Strengthening American Cybersecurity Act: What to Know and How to Comply https://papers.govtech.com/The-Strengthening-American-Cybersecurity-Act-What-to-Know-and-How-to-Comply-141446.html

1. 사이버 범죄-테러 통합정보센터 구축

○ 사이버 범죄-테러 관련 정보수집 및 통합 데이터베이스 구축

- 국가정보원 산하 "국가사이버안보센터 (NCSC: National Cyber Security Center)"를 중심으로 사이버 범죄-테러-에스피오나지 등에 대한 통합 데이터베이스 컨트롤타워 설치
- "국가사이버안보센터"를 선도 기관(즉 컨트롤 타워)으로 사이버 안보 관련 정보기관들과 수사기관들을 함께 묶는 정보공동체 구성
- 이 같은 정보공동체에는 다음과 같은 관련 기관들이 포함될 수 있음
  - · 군: 방첩사, 사이버사, 777부대, 정보사, 정보본부, 국방부 조사본부 등
  - · 정부부문: 검찰, 경찰, 해경, 외교부, 출입국외국인정책본부, 금융감독원, 국세청, 과학기술정보통신부, 방심위 등
  - · 공공부문: 한국인터넷진흥원, 국가보안기술연구소 등
- 국가사이버안보센터와 다른 범죄, 테러, 에스피오나지 등 관련 컨트롤타워 또는 데이터베이스 센터와의 연계성 강화
  - · 국가사이버안보센터와 테러정보통합센터 및 대테러센터의 연계강화
  - · 국가사이버안보센터와 방첩정보센터와의 연계강화
  - · 국가사이버안보센터와 검찰, 경찰, 보호관찰, 출입국관리국, 해경 등 수사 또는 형사사법기관들의 범죄정보센터와의 연계강화

○ 국가 통합정보센터를 허브로 전국 각 지역별 지역정보센터를 구축 서로 간 연계성 강화

- 국내 각 지역별 '합동사이버위협정보통합센터'를 설치하고 각 지역별 사이버안보 관련 기관들, 정보기관, 수사기관, 형사사법기관들, 관련 지방정부기관, 관련 민간기관들을 통합
- 이 같은 각 지역별 '합동사이버위협정보통합센터'는 다시 중앙의 '국가사이버안보센터'를 네트워크의 허브로 통합
- 각 지역별 '합동사이버위협정보통합센터'는 해당 지역의 사이버 범죄-테러-에스피오나지 관련 사안들의 정보를 취합 통합하여 중앙의 '국가사이버안보센터'로 전달하고, 반대로 중앙 컨트롤타워의 정보의 확산, 전파, 공유의 지역 거점으로 역할
- 각 지역의 '합동사이버위협정보통합센터'는 해당 관할 지역의 사이버 범죄·테러·에스피오나지 관련 여러 기관들을 선도하고, 조율하고, 지원하는 역할을 수행
- 각 지역의 '합동사이버위협정보통합센터'는 '국가사이버안보센터'가 직접 자금을 지원하고, 운용하며, 직접 관리 운용
- 각 지역의 '합동사이버위협정보통합센터'는 정보의 확산과 공유를 위해 매우 핵심적인 역할 수행
- 중앙의 '국가사이버안보센터'와 각 지역의 '합동사이버위협정보통합센터'는 긴밀히 연계 통합되어 사이버 공격위협으로부터 정부기관과 핵심기반시설들을 보호하고 보안을 강화하는 임무를 수행

○ 상시 통합정보 모니터링 및 분석

- 미국의 경우 NSA 신호정보부(Signals Intelligence Directorate)내에 메타데이터분석센터(또는 MAC)라는 24시간 감시센터를 구성, 운용
- 사업자가 고용 직원들의 이메일 포함 네트워크 트래픽 상시 모니터링

(개인의 프라이버시에 대한 예외, 미국 CISA 법)

- 민간 사업자에게 주기적 사이버 위협 평가의무 부여 (독립적 제3자 참여 필수)
- 필수적으로 사이버 위협을 모니터링하고 평가하는 자격 있는 사이버 위협 전담 임직원을 두도록 민간 사업자에게 의무화

○ 보호관찰과 교정국과의 정보협력체계 강화

- 보호관찰 대상이 되는 사이버 범죄자들에 대한 모니터링 강화와 국정원, 경찰 등과의 유기적 정보협력체계 구축
- 교도소에 수용된 사이버 범죄자들에 대한 모니터링 강화, 일선 정보수사기관과의 유기적 정보협력체계 구축
  · 해당 사이버 범죄자 출소 시 관할 경찰서와 국가사이버안보센터에 통지

○ 상황 발생 시 사건의 성격과 대응주체에 대한 결심판단

- 위기대응센터 설치, 운용
- 일반 사이버 범죄, 사이버 테러, 사이버 에스피오나지 등에 대한 판단 권한과 대응 절차, 대응 강도 등을 위기대응센터 컨트롤타워에서 결심 판단

2. 사이버 범죄-테러 대응을 위한 수사 전문성 강화

○ 진화하는 사이버 범죄 및 테러 양상에 맞춰 전문 수사교육기관 운용

- 미국의 경우 FBI의 사이버 수사-방첩 훈련학교를 미 해병대 콴티코 지기에 설치 운용
  · FBI뿐만 아니라 미국 내 사이버 수사-방첩 관련 거의 모든 연방, 주, 지방 수사기관들의 교육, 훈련을 전담, 전문성 강화
  · FBI의 사이버 훈련학교는 FBI의 정보수집과 처리, 그리고 보고를 총괄하는 작전기술과와 같은 공간에 위치, 상호간 연계성 강화, 이 같은 실무-교육의 연계성 강화를 통해 교육훈련의 질을 제고
- 미국 사례를 참조, 국내 국가사이버안보센터 산하에 사이버 범죄-테러 관련 수사전문 교육기관 설치 운용

○ 해당 전문수사교육기관에서 경찰, 검찰, 군, 정보기관 등 여러 관련기관 수사관들에 대한 통합교육 운용

- 미국 사례를 참조, 국내 국가사이버안보센터 산하에 사이버 범죄-테러 관련 수사전문교육기관을 경찰, 검찰, 해양경찰, 방첩사, 사이버사 등 관련 모든 중앙기관, 지방기관, 공공기관, 정부출연기관들의 사이버 범죄-테러-에스피오나지 관련 전문교육훈련기관으로 운용
- 해당 사이버 범죄-테러관련 수사전문교육기관에서 민간 수사전문교육센터를 개설 이와 연계하여, 민간 사이버 보안회사 및 민간 관련 전문가 양성을 위한 민간부문 통합 전문교육훈련 센터 운용
  · 정부부문과 민간부문의 사이버 범죄-테러관련 수사전문성 차별화와

보안 유지를 위해 정부 부문과 민간 부문을 격리하여 이원화 운용,

· 동시에 정부의 사이버 관련 수사전문교육훈련기관이 민간인들을 대상으로 한 민간 사이버 관련 수사전문훈련센터를 가이드하고 통제, 조율, 지원, 협력함

○ 사이버 전문인력 이외의 일반적인 수사관들과 경찰공무원들 대상으로도 사이버 범죄 및 테러 관련 기초교육 실시

- 일선 경찰 및 해양경찰, 중앙 및 지방 특별사법경찰관들을 대상으로 필요최소한 정도의 사이버 범죄-테러 관련 표준교육훈련 프로그램을 개발, 임용직후 기초교육훈련 및 승진·직무관련 교육훈련 프로그램에 커리큘럼으로 적용
  · 경찰의 경우 중앙경찰학교, 수사연수원, 경찰교육원 등
  · 군의 경우 장교, 부사관 기초훈련, 병과교육 등
  · 같은 정도로 해경, 보호관찰, 출입국외국인정책본부, 기타 특별사법경찰 등에 적용할 수 있음

○ 입법을 통한 수사 권한 강화

- 수사기관의 국내-기반 인터넷 서비스 공급자의 데이터에 대한 접근권한 보장 (미 CLOUD ACT)
- 수사기관을 위해 원격통신사업자와 제조업자가 필요한 감시(Surveillance) 역량을 지원하기 위해 시스템과 서비스를 구축하도록 법적 의무화 (미 Communications Assistance for Law Enforcement Act: CALEA)
- 민간 사업자가 자신들의 IT 시스템에 백도어를 설치하고 이를 수사기관이 활용할 수 있도록 엔크립션(encryption) 키를 수사기관에 제공하도

록 법적 의무화 (미 All Writs Act에 따라 몇몇 사례들에서 법원 명령으로 강제)

- 미국의 음모법(conspiracy law)을 한국에도 입법화할 필요

· 사이버 범죄-테러의 경우 오프라인의 조직범죄, 테러, 에스피오나지와 같이 범죄-테러 실행을 위해서는 음모(conspiracy)를 꾸미는 행위가 반드시 선행되어야 함

· 음모법은 범죄 행위와 별도로 이 음모행위 자체를 형사처벌의 대상으로 규정, 따라서 음모를 입증하기 위해서는 그 음모가 의도하는 범죄가 실제로 발생하였다는 사실을 입증할 필요가 없음, 즉 음모자체가 범죄를 구성하는 요건이 됨

· 음모법은 국가나 사회, 그리고 공공안전에 중대한 위협이 되는 모든 종류의 범죄단체 그 자체를 제거하기 위한 의도를 가진 법률, 즉 범죄자 개인이 아니라 범죄단체 자체를 제거하기 위한 의도를 가진 법률

· 음모법의 대상이 되는 범죄단체는 갱, 마약범죄집단, 모터바이시클 갱, 마피아, 극우, 극좌, 이슬람 등 다양한 테러조직, 해커 및 핵티비스트, 테러지원국가, 적대적 국가의 스파이 공작 네트워크 등 다양한 불법 조직, 단체를 두루 포함,

· 따라서 국내 n번방 성착취 동영상 거래조직, 해커조직, 스파이 네트워크 범죄조직, 불법 온라인 도박, 마약거래 등 다양한 사례에 적용될 수 있음

· 음모법이 성립하기 위해서는 둘 또는 그 이상의 개인들이 어떤 범죄행위를 실행하겠다는 동의(agreement)가 있어야 함, 여기서 범죄의 본체(corpus of the crime)가 되는 핵심사항은 '동의'의 존재여부, 즉 범죄를 실행하겠다는 동의가 있었다는 것을 입증하는 것만으로도 음모법으로 관련자들을 형사 처벌할 수 있음

· 동의의 존재여부는 수사관들이 입증해야 함, 하지만 그 동의가 목표로 하는 범죄가 실제로 완결되어야 할 것을 필요로 하지 않음
· 음모죄는 중간에 공모자들이 취소하거나 아니면 국가기관에 의해 방지되거나, 그 범죄의 완결자체가 애초부터 현실적으로 불가능했다는 이유로 그 죄가 면제되지 않음, 음모 가담자는 그러한 사실을 근거로 법적인 무죄를 주장할 수 없으며, 의도한 범죄는 완결하려는 진정성 있는 의도가 있었다는 사실만으로 음모죄로 처벌받을 수 있음
· 음모진행 과정에서 한 특정 공모자의 행동이나 발언은 음모에 연루된 모든 각각의 공모자들에 반한 증거로 법정에서 받아들여 짐
· 전문증거법칙(hearsay rule)의 중요한 예외
· 각각의 공모자는 각각의 모든 다른 공모자들이 저지른 모든 범죄들(음모진행 과정에서 그 음모가 목표로 하는 본질적 범죄결과와 관련 있는)에 대해 자신의 인지나 참여 여부와 관련 없이 책임을 짐, 이러한 원칙은 음모진행 과정 중 이후에 음모에 가담한 공모자에게도 적용

- 핵심데이터기반법(가칭) 입법
· 국가핵심기반시설(infrastructure security) 및 국가 핵심데이터 기반시설의 사이버 공격에 맞서 안전과 안정성 확보
· CDI(Critical Data Infrastructure) 시설들에 대한 특정 보안규정 도입
· 민간 CDI 소유자들은 자신들의 CDI 시설이 얼마나 중요한지 평가하고, 필요하다면 정부 레지스터에 등록 의무 부여
· 중요 CDI 시설 소유자들은 사이버 사건들을 예방하고 수사하는 데 있어 정부의 추가적인 보안요구들을 따르고 정부기관들과 협조의무 부과

- 가상사적네트워크(VPN: Virtual Private Network)법 입법

· 정보수사기관에 국내 웹사이트에 접근하는데 사용될 수 있는 수단제공
· VPN 솔루션 공급자들에게 정부와의 협력 의무와 국내에서 접근이 허락되지 않는 웹사이트들에 대한 사용자들의 접근 차단 의무 부과

- 인스턴트 메시지(IM: Instant Message)법 입법
  · 인스턴트 메시지 서비스 공급자들에 대해 특정한 규제부과
  · IM의 익명 사용 금지
  · IM 사용자들의 모바일 번호가 특정될 것을 지정
- 통신 운용자들(전화나 모바일 폰 서비스 공급자들과 같은)과 인터넷을 통해 정보를 배포하는 행위자들(인터넷 운용자들)에게 법적 의무부과
  · 모든 통신과 다른 사용자 활동들에 관한 데이터 저장 법적 요구
  · 통신 운용자들과 인터넷 운용자들에게 일정 기간 데이터 통신, 활동 등과 관련된 정보를 저장하도록 법적 의무부과
  · 인터넷 운용자들에게 정부기관의 요청에 따라 암호화된 데이터를 암호 해제하는 수단을 정부기관에 제공
  · 정부에 의해 허가된 암호해제 장비만을 사용하도록 규제
  · 통신 운용자들에게 사용자에 대한 정보보유 의무 부과
  · 권한을 부여받은 정부기관에 정보제공 협조의무를 통신 운용자들에게 부과, 반대로 특별히 대통령 명령으로 지정된 정부기관들에 인터넷 운영자들로부터 정보를 요청할 수 있는 권한 부여

○ 온라인 수색(또는 정부해킹, 합법해킹, 네트워크 수사기법)에 대한 수사역량 강화

- 국가기관이 기술적 수단(원격 통신 감시 소프트웨어)을 이용하여 이용자의 정보기술시스템에 비밀리에 접근하여 이용자의 시스템 이용을 감시하고 시스템에 저장된 내용을 열람하거나 수집하는 것을 말함
- 역량 있는 인원을 특채 또는 상시 채용 또는 헤드헌팅 등의 방식을 통

해 수사관으로 채용, 활용

- 온라인 수색 관련 교육, 훈련 강화

○ 생성형 AI(generative AI)가 초래하는 새로운 형태의 사이버 위협에 대한 수사역량강화

- 오정보/허위정보(misinformation and disinformation), 딥페이크(deepfakes), 자동화 허위조작정보(automated disinformation), 타깃 광고(Traget advertising), 데이터 프라이버시 우려(date privacy concerns), 소셜 미디어 알고리듬 조작(algorithmic manipulation of social media), 고도화된 피싱(sophisticated phishing), 생성형 AI에 대한 프롬프트(prompt) 인젝션 공격 등에 대한 수사역량 강화

○ 법제를 통한 잠입수사/비밀수사(undercover operations) 권한을 부여하고 관련 수사역량 강화

○ 원격 압수수색 및 온라인 수색에 대한 형사소송법상 근거 마련 및 판례를 통한 법률해석을 통해 합법화-활성화할 필요 있음

○ 온라인 수색, 추적, 탐지, 수사 전문팀 운용

- 기간 관 연계-협력을 통한 태스크포스 구성, 운용
- 미국 NSA 내 트랜스그래션 브랜치(Transgression Branch), 적대적 해커들을 추적하는 임무 수행
- 미국 NSA 내 TAO(Tailored Access Operations), 컴퓨터와 네트워크에 은밀히 잠입하는 데 필요한 맞춤형 도구와 기술들을 개발하고, 비밀작전

을 수행

- TAO 가운데서 최정예 엘리트로 구성된 원격작전센터(ROC: Remote Operations Center) 운용, 최고 수준의 은밀한 사이버 정찰, 감시, 공격임무 수행
- NSA는 CIA(Central Intelligence Agency)와 합동으로 특수정보국(Special Collection Service: SCS) 운용, 도청기지국을 운영, 커뮤니케이션 네트워크에 침입하기 어려운 곳에 NSA가 디지털 거점을 확보할 수 있도록 도와주며, 필요한 경우 그와 같은 시스템을 파괴하는 사이버 공격 감행
- NSA는 FBI(Federal Bureau of Investigation) 산하 데이터포착기술팀(DITU: Data Intercept Technology Unit)과 협력,
  · DITU는 NSA와 긴밀하게 협력, 미국 내 사이버 첩보활동이 제한된 NSA를 위해 대신 미국 내 국내 정보를 수집하거나 미국 내 기업과 민간부문으로부터 건네받아 NSA에 전달, 따라서 NSA가 미국 내 정보활동을 하지 않는 것은 맞지만 사실상 미국 내 정보활동을 수행
- 최정예 사이버 비밀작전조직 운용, 미국 CIA의 IOC, NSA의 TAO, FBI의 DITU 등
  · FBI DITU는 비컨(beacon)과 같은 해킹프로그램을 개발하는 데 관여, 연구와 실무의 시너지, 연계 강화
  · DITU는 비컨을 활용해 아동포르노 공급자와 같은 범죄자 추적과 사이버 방첩활동을 위해 해킹 수행, 특히 사이버 보안영역에서 FBI는 수사기관보다는 정보기관처럼 활동, 이들은 해커들을 법정에 세우는 일보다 앞으로 있을 공격을 예상하고 방어하는 데 더 큰 관심을 기울이고 정보를 수집, NSA나 다른 정보공동체 등에 전달하는 임무에 더 집중

· CIA의 정보작전센터(IOC: Information Operations Center)를 두고 사이버 수색-정찰과 정보, 방첩 등의 비밀임무를 수행

- 이 같은 미국의 사례를 참조하여, 국내 국가사이버안보센터를 컨트롤 타워로 국정원, 방첩사, 사이버사령부, 777사령부, 정보사, 경찰 국수본, 안보수사국, 검찰, 한국인터넷진흥원 등 관련 정보수사기관들의 주요 사이버 정보수사관련 부서들을 하나로 묶는 '기관 간 연계 태스크포스'를 설치하고

· 이를 플랫폼으로 정보-수사-비밀작전수행 기능을 하나로 통합하여 마치 하나의 기관처럼 운용,

· 이 경우 해당 태스크포스의 경우 마치 블랙박스처럼 처리되어 각 정보수사기관들에게 필요한 정보 또는 수사권한을 제공할 수 있으며, 국내 또는 해외, 군 또는 민간 등과 같은 각 개별기관의 관할권의 한계를 극복하고 관할권의 한계를 넘어 합법적으로 임무를 수행할 수 있도록 도울 수 있음

○ 범죄학자, 행동과학자, 심리학자 등이 참여하여 사이버 범죄자들에 대한 행동 프로파일링 및 관련 정보 데이터베이스를 구축

- 사이버 범죄자, 사이버 테러리스트 등에 대한 체계적 인간행동 프로파일링 조사
- 조사 결과의 데이터베이스 구축
- 사이버 범죄자, 사이버 테러리스트들에 대한 위험성 평가 분석
- 위험평가를 기초로 한 선제적 대응 필요성 평가
- 사이버 범죄자, 사이버 테러리스트들에 대한 행동특성에 관해 사이버 대응 실무자들을 지원

- 예를 들면, 사이버 범죄자, 사이버 테러리스트들의 행동특성을 다음과 같은 목적에 따라 프로파일링 할 수 있음
  · 금전을 목적으로 한 사이버 범죄 (해킹을 통한 정보 불법거래)
  · 감정적 동기를 위한 범죄 (사이버 스토킹)
  · 성적 동기에 의한 범죄 (디지털 성착취물)
  · 정치적 동기에 의한 범죄 (사이버 테러)
  · 위험성 정도가 낮은 범죄 (영화, 소프트웨어 등에 대한 저작권법 위반)
  · 사이버 에스피오나지

3. 사이버 범죄-테러 피해에 대한 신속 지원체계 강구

○ 공공의 사이버 범죄-테러에 대한 인식 고취

○ 사이버 범죄에 대한 저항성을 강화하기 위해 일반 국민을 대상으로 한 사이버 보안의식 교육 및 캠페인 추진
  - 오늘날 사이버 범죄-테러 피해에 대한 저항성을 의미하는 사이버 역량 격차를 'CPL(Cybersecurity poverty line)'로 부름
    · CPL에는 사이버 기술의 격차, 사이버 보안 인력과 기술, 시스템에 투입되는 비용에 더불어 보안(security)에 대한 사회경제적 태도의 격차도 중요한 지표 가운데 하나로 포함
  - 따라서 CPL을 기준으로 이로부터 상당 정도의 상위 수준을 유지하기 위해서는 일반 국민 대상의 광범위하고 체계적인 사이버 보안의식 교

육 및 캠페인이 필요함

· 이를 통해, '보안에 대한 사회경제적 태도'의 수준을 높일 수 있음

- 유치원부터 초·중·고·대학교 과정에서 필수 과목으로 체계적 교육이 요구됨
- 사회문화강좌, 방송, 유튜브 등을 통한 전국민 대상 광범위하고 체계적인 사이버 보안 교육이 필요함

○ 사이버 범죄-테러 피해 신고 센터, 즉 '원스탑 센터' 운용

- 신고절차 간소화
  · 신고자의 이름과 연락처
  · 피해사실과 관련 개인정보
  · 피해일자와 피해규모
- 스미싱, 해킹, 디도스, 앱 이용금융사기, 온라인 성착취물 등 모든 생활밀착형 온라인/사이버 범죄 의심사례 또는 피해사례 문의, 신고 절차 간소화 (원스톱 센터 운용)
- 국내에서 성범죄 관련 사건에서 운용되고 있는 '해바라기센터'를 참조할 필요가 있음
  · 해바라기센터는 성폭력, 가정폭력, 성매매피해자 등에 대하여 365일 24시간 상담, 의료, 법률, 수사지원을 원스톱으로 제공함으로서 피해자가 폭력피해로 인한 위기상황에 대처하고 2차 피해를 방지할 수 있도록 지원하는 기관
  · 현재 해바라기센터는 전국에 39개소가 운용 중으로, 2024년까지 2개소를 확충할 계획
  · 취약층 범죄피해자(예를 들면 미성년 피해자 등)의 2차 범죄피해와 법정

출석 등을 지원하기 위해 인력과 장비, 시설을 배치, 운용

· 범죄 신고와 피해자 지원 기능을 통합하여 원스톱으로 지원, 운용

· 상담, 의료, 수사, 법률지원, 심리치료까지 각 부문별 전문가들을 배치하여 응급상황에서 사후 치료 및 지원 등에 이르기까지 원스톱으로 피해자 지원

· 피해자 중심 수사를 지향

- 이 같은 국내 성범죄 관련 해바라기센터의 긍정적 사례를 참조, 사이버 범죄-테러 부문에서 신고, 응급상황대응지원, 사후 법률지원, 상담, 피해복구 등에 이르는 범죄피해 신속지원체계의 원활화를 위해 해바라기센터에 준하는 원스톱 시스템을 설치, 운용할 필요 있음

○ 사이버 범죄-테러 피해 통보 의무화

- 사이버범죄-테러 피해 발생 시 해당 사실을 개인에게 통보하도록 민간 사업자에게 의무화 (미국의 경우 통보 타임프레임이 30일 이내임)
- 피해사실 수사진행상황과 피해복구상황, 구제절차 등에 대해 피해당사자 개인에게 통보 의무화 (미국의 경우 통보 타임프레임이 30일 이내임)
- 댐, 교통시스템, 핵심 제조업 등을 포함하는 핵심기반시설 (critical infrastructure) 운영자에게 모든 사이버 침해사건 발생 인지 시 72시간 내에 국가사이버안보센터(NCSC)에 통보하도록 법적 의무화 (미 Strengthening American Cybersecurity Act 참조)
- 랜섬웨어 지불을 한 조직에게 지불요구 액수, 강요된 지불방법, 실제 지불된 금액 등을 포함하는 지불 상세내역을 24시간 내에 보고하도록 법적 의무화 (미 Strengthening American Cybersecurity Act 참조)

○ 사이버 범죄-테러 피해복구 및 피해자 지원 태스크포스 운용

- 온라인을 통한 사이버 범죄 발생 시 대응절차와 피해복구, 피해자 지원 절차 등에 대한 가이드라인 제공
- 검찰 경찰, 지방정부, 지역 변호사회, 민간 사이버 보안 회사, 지역 피해자 지원센터, 금융기관 등과의 피해자 지원 파트너십 구축
- 사이버 범죄-테러 수사-기소-재판 절차에 범죄피해자의 적극적인 참여 시스템 구축
  · 범죄 피해자의 정서적 만족도 증대
  · 범죄 피해자의 권리 증대
- 무료 피해자 지원 자문 기구설치, 운용

○ 사이버 범죄 피해 취약계층을 중심으로 온라인 및 오프라인 커뮤니티를 형성하고, 커뮤니티 기반 피해예방, 피해복구, 피해자 지원체계 구축

- 피해 발생 시 피해자의 대응행동요령에 대한 표준대응절차를 마련 운용
- 표준대응절차 마련을 위한 행동과학적 연구, 조사, 결과 도출 필요
- 피해자에 대한 '의사결정지원' 체계 마련 및 지원
- 생성형 AI 기반으로 사이버 범죄 피해 발생 시 피해자의 행동요령, 의사결정방안 등에 대한 지원

○ 사이버 범죄 피해자 구호 기금 조성

- 사이버 범죄자들로부터 압수한 자금의 일정 부분을 이용, 기금 조성

○ 사이버 침해 피해에 대한 사이버 보험(cyber insurance) 운용 지원, 제도화

- 랜섬웨어 공격 등에 대한 랜섬(ransom) 지불

- 소송 비용, 수사 비용, 그리고 피해에 대한 구제 등
- 사이버 보험 산업이 급격히 증대함에도 중소기업, 영세기업, 비영리 민간조직 등은 사이버 보험의 보호의 사각지대에 있음
  · 예를 들면, 100,000명 이상의 직원을 가진 조직의 85%가 사이버 보험을 들고 있는데 반해 250명 이하의 조직의 21%만이 사이버 보험 정책을 갖고 있음
- 사이버 보험은 사이버 회복력의 확보에 있어 가장 핵심적 요소 가운데 하나
- 사이버 보험의 투명성(transparency) 제고
- 사이버 보험 생태계 구축

○ 민간 부문의 사이버 회복력(resilience) 강화
- 오늘날 민간 부문의 사이버 회복력은 양극화되고 있으며, 사이버 회복력의 격차가 민간 부문의 경제 역량 격차에 결정적 영향을 미치고 있음
- 생성형 인공지능(generative AI) 같은 새기술이 사이버 회복력의 양극화에 결정적 영향을 미침, 따라서 생성형 AI가 사이버 침해 위협으로부터 방어를 위한 핵심 역량이 되고 있음
- 민간 기업과 조직 등 민간부문의 사이버 회복 역량의 불평등성을 개선할 수 있는 체계적인 해결책을 정부가 지원해야 함
  · 특히 중소기업과 비영리 민간조직, 단체 등 취약 민간부문에 대한 사이버 회복력을 지원할 필요 있음
- 오늘날 대기업과 중소기업 사이의 사이버 회복력 격차는 사이버 생태계의 상호연계성을 고려하면 매우 심각한 사안
- 민간 부문 사이버 회복력 강화를 위한 인력 확보

· 전문 인력 자격 요건에 해당하는 전통적인 대학 또는 대학원 학위 과정 이외에 단기간에 걸친 훈련 프로그램과 자격증 인증 등의 시스템을 통해 전문 인력의 양과 질을 확충, 보강

· 전문 인력 양성을 위한 다중이해당자사주의(multistakeholderism) 접근, 정부, 민간, 학계, 기업 등이 사이버 전문 인력 양성을 위해 합동 프로그램 개발·운용

- 공급망 안전을 위한 사이버 회복력 확보

○ 회복적 사법체계 구축

- 사이버 범죄-테러 신고 이후 피해자들이 주요한 참여자로 이후 수사-기소-재판 절차에 참여 기회 부여
- 특히, 재판 시 형 확정과 양형판단에 피해자들의 목소리가 반영될 수 있도록 함
- 피해자는 정당하고 납득할만한 가해자에 대한 처벌이 있을 때 범죄 피해의 트라우마를 극복할 수 있음

4. 사이버 범죄-테러 기관 간 공조 강화

○ 범정부간 공조 강화

- 미국 사례 참조

· NSA와 사이버 사령부의 수장을 통시에 NSA 수장이 겸임함으로서 평시 사이버 정보-방첩활동과 전시 사이버 전쟁수행을 유기적으로

통합

· NSA와 DIA(Defense Intelligence Agency) 소속 해커들을 함께 '수색팀' 구성, 운용

- 국가사이버안보센터, 경찰, 방첩사, 사이버사, 검찰, 보호관찰, 교정, 출입국, 한국인터넷진흥원 등 관련 기관들 간의 공조 강화
- 국가사이버안보센터를 선도기관으로 하는 범정부 정보공동체 구축

○ 정부-민간 간 공조 강화

- 민간 기업의 사이버 공격 위협 탐지 역량을 활용
- 미국의 CISA(Cybersecurity Information Sharing Act) Law 도입

· 민간 기업의 자체 방어역량 강화를 포함한 네트워크 트래픽 감시능력 강화

· 민간과 정부 부문 간의 사이버 위협 정보 공유 촉진

- 미국의 경우 CISA(Cybersecurity and Infrastructure Security Agency) 설치, 이를 통한 핵심기반시설 보호 및 민간-정부 사이의 조율, 위협 정보의 민간 부문 제공
- 미국의 경우 SACA(Strengthening American Cybersecurity Act)를 통해 정부기관들 간의 소통과 조율을 증진시키고 사이버침해사건 정보의 공유 법적의무 부여
- 민간 부문, 특히 핵심기반시설 운용 민간 사업자의 "중대한 사이버 침해사건(significant cyber incidents)" 정부 보고 의무화, 법률적 강제조항 (CIRCIA: Cyber Incident Reporting for Critical Infrastructure Act of 2022)
- 정부와 민간부문간의 2단계 공조시스템을 구축

· 미국의 경우, NSA를 핵심 컨트롤타워로 AT&T, 버라이즌, 센추리링

크와 같은 대형 인터넷 공급자나 네트워크 운영자를 티어 1(Tier 1)으로 참여시켜 민간 컨트롤타워로 구축, 여기에 티어 2(Tier 2)에 해당하는 기타 민간기업들을 참여시켜 확장 보안 시스템을 구축

· 한국의 경우, 국가사이버안보센터를 핵심 컨트롤타워로 KT, SK, LG U+ 등 대형 인터넷 공급자와 네이버, 카카오 등 대형 포탈 등을 티어 1(Tier 1)으로 참여시켜 민간 컨트롤타워로 구축, 여기에 티어 2(Tier 2)에 해당하는 기타 사이버 보안기업들을 포함한 민간기업들을 참여시켜 확장 보안 시스템을 구축

○ 사이버 범죄-테러 관련 민간에 법적 의무부과

- 수사기관에 (민간 사업자에 대한) 가입자 정보에 대한 제출명령권 부여
- 현행 전기통신사업법 83조 4항 규정을 임의규정에서 강제규정으로 전환 필요
  · 민간 사업자에 대한 수사기관의 통신자료 요청에 대한 민간 사업자의 협력 강제
  · 현재는 통신자료 수집의 경우 형사소송법에 따른 압수수색검증영장을 발부 받아 시행
  · 전기통신사업법에 따른 통신자료 요청 강제화 필요
- 민간 사업자에 대해 트래픽 데이터와 위치정보에 대한 제출명령 규정
- 민간 사업자에 대해 콘텐츠 데이터의 감청에 대한 기술지원을 제공 의무 규정
- 민간 사업자에 수시기관이 통신내용을 획득하도록 수사기관에 기술적 지원을 제공하도록 의무 규정
- 이와 같은 법적 의무 부과된 민간 행위자는 대한민국 영토 내에서 전기

통신네트워크를 통해 신호를 전달하거나 이용자로 하여금 전기통신네트워크를 통해 정보를 얻고, 수신하거나 유포할 수 있게 해주는 서비스 제공자 및 전기통신네트워크 운영자에게 적용

- 협력 의무가 있는 민간 사업자가 해외에 있는 경우에도 국내에서 서비스를 제공하고 있을 경우 동일하게 적용되도록 법제와 판례를 통해 강제
  · 즉, 한국과의 충분한 영토적 관련성을 인정하는 결정적인 요소는 서비스 제공자의 사무실이나 설립지의 위치가 아니라, 서비스 제공자가 서비스를 제공하는 장소라는 원칙 확립 필요

○ 민간 사이버 탐정 역량 구축 및 활성화

- 민간 온라인 수사 법제화 및 활성화
- 민간 사이버 침해 행위에 대한 현상금 사냥꾼(Bounty Hunter) 활용
  · '바운티 헌트'는 영리를 목적으로 범죄 또는 범죄자를 수사, 추적하는 민간 수사관(또는 사설 탐정)
  · 사이버 공간상에서 사실상 효과적인 범죄-테러-에스피오나지 감시, 순찰(patrol)이 되지 않는 실정을 고려 민간 역량을 최대한 활용할 필요 있음
  · 경찰, 검찰 등 기존 공권력만으로는 사이버상에서 효과적인 범죄 감시와 순찰활동이 어려움, 이는 인적, 물적 역량의 한계 때문
  · 상황범죄이론(situational crime prevention: SCP)에 따르면 범죄는 동기화된 범죄자(motivated offender), 적절한 피해대상(suitable victim), 그리고 보호자의 부재(absence of the guardians)라는 세 요인이 같은 시간과 같은 공간에서 맞아 떨어지기 때문임, 사이버 공간은 대표적인 사례임, 다수의 동기화된 범죄자와 적절한 피해대상이 같은 공간-시간

때에서 만나며, 동시에 경찰, 검찰과 같은 보호자의 만성적 부재가 나타남

· 따라서, 민간의 사이버 침해 위협 탐지와 조사 역량을 최대한 활용할 필요 있음

○ 민간 사이버-범죄 테러 신고제도 활성화

- 민간 네티즌의 사이버 범죄-테러-에스피오나지 신고제도 활성화를 위한 원스톱 신고 센터 운용
- 앞서 제시한 것처럼 피해신고와 피해자 지원, 구제를 결합한 원스톱 시스템을 설치 운용할 필요 있음
- 민간 사이버 침해행위 신고에 대한 포상금 기준 마련 및 실행
  · 포상금의 액수를 크게 하는 것보다 적정액의 포상금의 지급의 확실성(certainty)을 높이는 것이 바람직함
  · 실제 포상금 지급 사례 등을 적극적으로 홍보하여 사이버 범죄-테러 신고 시 실제 보상을 이어진다는 점을 대중들에게 인지적으로 각인시킬 필요 있음

5. 사이버 범죄-테러 대응 국제협약 가입

○ 다자간 사이버범죄 대응 공조협약 가입 추진

- 2022년 10월 유럽평의회 사이버범죄 협약(부다페스트 협약) 가입의향서 제출

- 유럽평의회는 심의를 통해 2023년 2월 8일, 부다페스트 협약 가입을 위해 우리나라를 초청
- 한국이 사이버 범죄 협약에 가입하게 되면 협약의 국내적 수용을 위한 이행입법을 마련해야 하므로 협약의 절차법 조항과 한국의 형사소송법, 통신비밀보호법 등 관련 조항을 제·개정할 필요 있음
- 가입을 위한 초청은 이후 5년간 유효하며, 한국 정부는 협약 비준을 위한 국내 절차가 완료되면 가입서를 기탁할 예정임
- 협약 가입절차를 완료하기 위해 사이버 범죄 협약의 이행 입법을 마련하여야 함
- 사이버 범죄 협약 당사국인 주요 국가의 법제 연구, 전기통신 사업자 등 서비스 제공자, 학계, 전문가, 시민사회, 정치권 등 이해관계자의 의견을 충분히 수렴, 검토하여 국내 법제 정비 필요

○ 부다페스트 협약 가입 - 외사 공조

- 형사소송법 개정을 통해 수사기관이 서비스 제공자에 통신데이터 제공을 요청할 수 있는 근거 규정을 둘 수 있음 (벨기에 사례)
- 서비스 제공자의 협력 의무 역시 규정할 수 있음 (벨기에 사례)
  · 벨기에 형사소송법은 인터넷 서비스 제공자에 대하여 사법기관 협력 의무 부과, 불이행시 형사처벌
- 유럽평의회(Council of Europe) 사이버 범죄 협약 19조 2항은 원격 압수수색 (remote access)을 규정
  · 따라서, 이에 대응한 해킹 등 기술적인 수단을 이용한 온라인 수색 가능
  · 협약 가입을 통한 국내 법제 마련을 통해 원격수색과 법적 해킹, 그

리고 데이터 감청 등의 사안들을 입법화

· 합법적 해킹의 경우 살인, 인신매매, 성범죄, 테러리즘과 같은 중범죄가 발생하였을 것이라는 확실한 정황이 있어야 하고, 이러한 조치가 실체적 진실 발견을 위해 필요한 것이어야 하며, 해당 조치의 대상이 피의자이거나 피의자와 정기적으로 연락을 하는 자일 것이라는 제한 조건을 둘 수 있음

- 민간 정보통신 사업자의 통신데이터 등에 대한 접근을 위해 관련 이해당자국들과의 국제사법공조 강화 (양자 및 다자협약)

○ 사이버 범죄-테러를 모멘텀으로 한 한국의 중견국 외교

- 한미 동맹을 사이버 공간으로 확대, 사이버 공간에서의 한미동맹 구축
- 한-나토 간의 사이버 안보에 대한 결속 공고화, 나토 조약 5조(다른 나토 회원국이 적의 공격을 받을 경우 이를 동맹 전체에 대한 공격으로 간주, 다른 동맹국들이 공동 대응에 나선다는 규정)가 사이버 공격에 한하여 한국에 적용되는 정도로 추진 노력
- 미국 및 다른 서방 국가들이 주장하는 글로벌 하나의 인터넷, 정보의 자유로운 소통, 표현의 자유 등에 기반을 둔 사이버 국제규범 구축에 동참
- 동시에 글로벌 인터넷이 미국 주도의 서방 인터넷 권역과 중국-러시아 등의 권위주의 체제 인터넷 권역으로 사이버 공간이 분리될 것에 대비, 한국과 유사한 입장에 처한 유사입장국들(like-minded countries)과의 연대 및 소통 강화

· 이를 위해 한국과 핀란드, 스웨덴, 에스토니아, 오스트레일리아, 뉴질랜드, 독일, 프랑스 등 미국과 입장을 같이 하면서도 동시에 러시아-

중국 등으로부터의 압력을 받고 있는 유사입장국들과 연대-협력

· 중앙아시아 5개국, 몽골, 동유럽 국가들 등 한국에 문화적으로 우호적인 국가들을 대상으로 한국의 정보통신, 인터넷, 경제협력, 과학기술, 사이버 안보, 사이버 수사역량, 법제도 등을 지렛대로 연대와 협력 형성, 양자 간 및 다자간 협력 체제 강화

· 중동, 동남아 및 남아시아 국가들을 대상으로 반중 또는 중국에 대한 위협 인식 기조를 지렛대로 한국 주도의 양자, 다자간 협력-연대 추진

○ 요약하면, 정보-수사-피해지원-회복력 등의 사이버 탐지, 예방, 대응, 복구 역량 강화가 통합적으로 이루어질 필요 있음

- 정보기관 간 유기적 협력체계 구축필요

· 정보공동체 구성기관들을 하나로 묶고 기관 간 정보의 공유-통합을 강화

· 정보-수사의 일련의 대응 과정 또는 절차를 유기적으로 연계-통합

- 다중이해당사자주의에 기초하여 정부-민간의 유기적 협력 체계 구축

· 민간이 사이버 침해위협 대응의 적극적 주체이자 파트너가 되고 이를 정부-군이 지원, 협력하는 체제구축

- 국제적 연대와 협력강화를 위해 부다페스트 협약 가입 추진

○ 향후 전망의 시각에서 보면, 생성형 AI, 퀀텀컴퓨팅, IoT, 드론, 로봇, 뉴로사이언스, 메타버스, 3D 프린팅 등 신기술의 상용화가 가속되면서 기존의 사이버 위협이 이 같은 신기술과 접목되어 더욱 복잡하고 치명적으로 진화할 개연성이 큼

- 신기술과 접목되어 진화하는 사이버 범죄-테러 위협에 대한 예측과 평

가, 대응 방안의 선제적 노력이 요구됨

- 사이버 범죄-테러 부문에서 개인과 민간조직, 단체 등과 민간 부문의 기술적 역량이 급격히 증대할 것으로 보이며, 따라서 민간 부문의 위협이 심각해질 것으로 예상
- 이 같은 민간 부문이 초래하는 사이버 범죄-테러의 위협이 중국, 북한 등 국가적 위협 행위자와 결합되면서 점점 더 민간의 범죄-테러 위협과 국가적 에스피오나지·정보공작·전쟁의 위협이 융·복합 될 것으로 보임
- 생성형 AI 등 새로운 기술의 급격한 발전으로 개인들 간의 사이버 역량 격차가 급격히 더욱 심화될 것으로 보임
  · 이 같은 위협은 사이버 역량을 가진 소수와 사이버 역량이 결핍된 대다수로 나뉘는 사이버 역량 양극화가 극심해 질 것임
  · 이 때문에, 사이버 역량을 결핍한 대다수 피해 대상자들에 대한 사이버 역량을 가진 소수의 범죄-테러 가해는 더욱 심해지고 그 위협도 더욱 증대할 것으로 보임
  · 더욱이 기술의 빠른 발전으로 사이버 전문 인력을 양성하고 확보하는 것이 더욱 어려워질 것으로 보여 사이버 역량을 갖춘 악성 행위자들을 막을 사이버 전문인력의 부족 현상이 문제가 될 것으로 보임

제4장

사이버 안보 기술역량 강화 및 공급망 안보 확보

유 인 태 | 단국대학교 정치외교학과 조교수

1. 기술개발과 공급망 재편과 관련된 국제협력
2. 범국가적 공급망 사이버 안보 정책 및 대응체계 확립
3. 국가 사이버 안보 대응 산업·기술 역량 강화
4. 사이버 안보 관련 기반 기술의 전략산업화
5. 신흥기술에 대한 사이버 위험 관리체계 확립

제4장

사이버 안보 기술역량 강화 및 공급망 안보 확보

유 인 태 | 단국대학교 정치외교학과 조교수

배경과 구성

- 제4장은 <국정과제>, <국가안보전략>, <국가사이버안보전략> 등을 검토하고, <국가사이버안보전략>에 이어 사이버 안보 전략을 구체화 및 이행하기 위해 만들어질 <국가사이버안보기본계획>과 <국가사이버안보시행계획>의 차원에서 연구를 수행하고 정책을 제시함
- 글로벌 공급망의 사이버 안보 위협 대처를 위한 국제협력, 공급망 사이버 안보, 사이버 안보 인재 육성 및 산업 역량 강화, 그리고 신흥기술의 사이버 위협 등 다섯 가지 주요 아젠다를 논의함
- 한국이 추진하고 있는 관련 정책, 규제, 프로그램들을 우선적으로 검토하고, 향후 전망과 그에 의거한 정책 제언을 함

- 제4장의 구성은 다음과 같은 다섯 가지 항목을 중심으로 함
  1. 기술개발과 공급망 재편과 관련된 국제협력
  2. 범국가적 공급망 사이버 안보 정책 및 대응체계 확립
  3. 국가 사이버 안보 대응 산업·기술 역량 강화

4. 사이버 안보 관련 기반 기술의 전략산업화

5. 신흥기술에 대한 사이버 위험 관리체계 확립

1. 기술개발과 공급망 재편과 관련된 국제협력

○ 글로벌, 소다자 및 지역 그룹 및 전략에서 기술개발, 공급망 재편 논의가 미국과 미국의 동맹국 및 파트너 국가들 간에 중요하게 이루어지고 있음

- G7에서의 2023년 '공동선언'에서는 기술 유출과 경제적 강압을 우려하며, 복원력을 강조하고 있음. 이러한 측면들은 모두 기술개발협력과 공급망 재편으로 이어지고 있음
- 미국-EU 무역기술위원회(TTC)에서도 수출통제작업반을 통한 글로벌 공급망 재편을 꾀하고 있으며, 쿼드(QUAD)에서도 핵심신흥기술 표준에 대한 공동원칙을 내놓고 있음. 오커스(AUKUS)에서도 미국의 수출통제체제를 도입하며, ITAR에 의해 통제되는 핵, 우주 기술 등 수준 높은 기술들의 이전을 위해 회원국들이 국내 체제를 정비해 나가고 있음
- 바세나르 체제 등, 글로벌 수출통제체제에서의 개혁의 목소리가 나오고 있음. 미국이 적성국가로 지정하는 국가들을 제외하고, 미국의 동맹 및 파트너 중에서도 기술적 우위와 상호운용성을 기반으로 한 국제협력이 가능한 나라들 중심으로 재구성되는 방향으로 추진될 수 있음

○ 한국은 인도태평양 전략을 통해 미국, 일본 및 인도-태평양 국가들과 공급망 안보와 사이버 공간의 안전과 신뢰성 확보를 위한 협력을 강화하기

로 하였음

- 미국과 같은 기술 선진국과는 기술개발 및 표준 협력 그리고 동남아시아 국가들에게는 사이버 역량 강화 지원(CCB)의 방향성을 표방함
  · 2024년 3월 과기부는 세계은행과 디지털 개발 분야 협력을 위한 MOU를 체결함. 2021년부터 디지털개발 3개년 협력 프로그램('한국 디지털개발프로그램')의 일환이며, AI, 데이터, 사이버보안 관련 한국의 주요 정책을 공유하고, 디지털 혁신 사례와 디지털 신질서 정립 방향을 발표함
- 2021년에는 최초로 '세계신안보포럼'이 1.5트랙 회의로 개최되었으며, 사이버안보, 보건, 안보, 신기술 안보 3개 세션으로 개최되었음. 2024년까지 개최되었음
- 2024년에는 한국이 3월 '민주주의 정상회의'를 주최하며 AI 논의를 갖고, 5월 AI Seoul Safety Summit, 9월에는 '인공지능의 책임있는 군사적 이용에 관한 고위급회의(REAIM)', 12월 AI Summit Seoul 등을 개최함.

○ 2022년 윤석열 정부 출범 이후 국제협력, 첨단기술 개발, 공급망 재편의 맥락에서 사이버안보 아젠다가 활발히 추진됨. 2024년 국가 사이버안보 전략서에서도 첨단기술 협력의 맥락에서 사이버안보가 강조됨

- 2024년 9월 11일 처음으로 개최된 '사이버 서밋 코리아(CSK) 2024'에서 한국을 인도태평양 지역을 대표하는 국제 사이버 훈련 허브로 발전시킬 계획을 발표함
  · 국가·공공기관에서 사용하는 암호모듈의 안전성을 검증하는 '암호모듈 검증제도'(KCMVP)에서 국제표준암호인 AES를 허용하기로 개정하였음. 이로써 수출 경쟁력 약화와 개발 효율성 저하 문제가 해소

될 수 있을 것으로 보임.

- 우방국과의 사이버 공조 강화도 추진되고 있음
  · 2022년 미 바이든 대통령의 방한은 정책결정자들의 첨단기술에 대한 달라진 관심 정도를 반영하듯 삼성전자 평택 고덕 캠퍼스에서 시작하였으며, 핵심 신흥 기술 보호 및 진흥 그리고 사이버안보를 위한 민관 협력에 합의함
  · 2023년 4월 한미정상회담에서의 워싱턴 선언은 핵심신흥기술, 경제안보, 사이버안보 등을 포괄했으며, 한미동맹을 사이버 공간으로 확장하는 '사이버 안보 협력 프레임워크'가 채택되었음
- 이하에서 언급하듯, 법제도 정비와 구체적 실행 계획 수립 과제 등이 남아 있음

○ 2023년 12월 산업통상자원부는 '글로벌 기술협력 종합전략'을 발표하고, 2024년 1월에는 '2024년 산업기술국제협력사업' 통합 시행계획을 공고하였음

- OECD에 따르면 한국이 세계 최고 수준의 R&D 투자에도 불구, 국내 R&D 성과가 여전히 미흡한 이유로, 국제 공동연구 저조를 지적함
  · 글로벌 협력으로 신기술 개발의 리스크를 낮추고, 규범, 표준의 선점이 필요함. 그리고 이에 따라 안정적 공급망 확보 가능성이 커짐
- '종합전략'에 따라 2024년 국내 기업을 위한 장기적이고 안정적인 협력 통로 구축 및 차세대 산업원천기술 확보를 위해 '글로벌 산업기술협력센터' 사업이 신설되었음
  · '종합전략'에 의한 2024년 지원 규모는, 전년(1,061억 원) 대비 56%(598억 원)를 확대 편성한, 총 1,658억 원이며, 연구 지원 규모는

과제당 최대 100억 원임

- '종합전략'에서는 '초격차 급소기술', '차세대 산업원천기술', '도전적 미래기술' 그리고 '기업의 수요맞춤형 요소기술' 등으로 전략기술을 구분하고 있음. '초격차 급소기술'의 경우, 80개 핵심(급소)기술을 선정하고, 산업부 R&D를 외국기관에 전면 개방하여 국제협력을 통해 기술 확보를 추진하고자 함.
  · '종합전략'은 우방국 중심의 전략적 기술협력 기반 구축을 표방함. 미국, 유럽, 일본, 아세안을 언급함
  · 후보기술을 선정하고, 후보 파트너 기관을 조사하고 있으며, 개발 기간을 예상하고 있음

○ 향후 동지국가(like-minded countries) 간 기술 공급망을 지속 또는 강화하는 방향은 계속될 것임

- 기존의 양자 또는 소다자 차원의 기술 연대의 정도와 범위가 확장될 수 있음
  · 이미 첨단뿐 아니라 레거시 반도체 기술들도 포함하는 더 많은 기술들을 포함하는 방향으로 움직이고 있으며, 아직은 본격화되지 않은 우주나 바이오와 같은 기술 부문들도 포함될 수 있음
- 또한 다자수출통제체제에서도 동지국가간 기술 동맹으로 재편될 수 있음.
  · 현행, 이중용도 관련한 바세나르협정은 중국이나 러시아와 같은 국가들도 포함하고 있으나, 이들을 배제한 글로벌 다자수출통제체제가 부상할 수 있음
- 이러한 기술 연대의 움직임에서 기술 표준이나 기술 사용에 있어서의

규제나 법을 통해, 사이버보안에 대한 표준을 같이 형성해 나갈 수 있음

· 실제 EU의 GDPR은 데이터 프라이버시에 관련한 규정이나, 데이터 보안과 관련한 보안 표준을 준수할 수 있도록 대기업뿐만 아니라 중소기업에도 압박이 되었음

- 따라서, 향후 첨단 기술과 관련한 국제적 논의에 사이버보안 전문성을 갖춘 인재가 같이 참여하여 국제적인 논의를 이해할 수 있으며, 한국의 사이버보안 표준의 우수성을 적극 알릴 필요가 있음

· 관련하여 국제 사이버안보 레짐 형성의 동향을 지속적으로 파악해야 함

2. 범국가적 공급망 사이버 안보 정책 및 대응체계 확립

○ 공급망 사이버안보에 대한 위협이 강조되고 있으며, 이에 대한 대처의 요구가 부상하고 있음

- 중국 화웨이의 5G 네트워크 장비는 대표적 예이며, 국내에서 시작된 공급망 사이버안보에 대한 위협인식이 아니더라도, 미국 또는 EU발 위협인식이 국내 정책의 변화를 압박할 수 있음.

· 동맹국 또는 파트너 국가로서 그러한 위협 인식에 대해 어느 정도 안심시킬 수 있는 외교적 대응 또는 국내 조치가 필요한 현실이 도래한 바 있으며, 앞으로 더욱 그러할 가능성이 커지고 있음.

· 차세대 네트워크 장비, 6G나 ORAN과 관련해서도 제기될 수 있으며, 적성 국가를 통해 제조 또는 공급되는 여러 종류의 재화와 서비스에

대해 제기될 수 있음.

- 미국에서는 2023년 3월부터 본격적으로 제기된 ZPMC(Shanghai Zhenhua Heavy Industries, 중국명 '상하이전화(上海振華)중공업')의 대형 크레인은 또 다른 예임.
  · 같은 해 이슈가 되었던 미래 자동차의 핵심 기술 중 하나인 라이다(LiDAR)도 레이저 센서 기술이며 민감한 이중용도 기술이기 때문에, 미국의 이에 대한 안보 우려가 커지고 있음.
  · 중국산 DJI 드론 그리고 틱톡(TikToK)과 같은 소셜네트워크 서비스에 의한 데이터 유출 우려는 모두 공급망 사이버안보 정책의 강화 필요성을 제기하였음.
  · 그 외에도 중국의 커넥티드 차량(connected vehicle)이나 쉬인, 핀둬둬, 테무, 알리페이 앱과 같은 전자상거래(e-commerce) 관련 플랫폼들이 이미 행정명령이나 법안에 포함되어 있어서, 국제적 이슈가 될 잠재력을 보이고 있음
  · 산업과 부문을 넘어, 적성 국가로 지정된 통해 제조 및 유통되는 재화나 서비스에 폭넓게 공급망 사이버안보의 우려가 국제적으로 제기될 소지가 크며, 한국의 대응 및 조치를 요구할 가능성이 커지고 있음
- 한국에서도 화웨이 5G 장비 사용에 의한 보안 위협, 공공기관의 중국산 CCTV 및 보안장비 사용, 대기업들이 사용하는 중국 및 외국산 IT 장비와 소프트웨어 사용, 그리고 철도 시스템에서 사용하는 중국산 장비를 통한 해킹 시도로 철도 운행 데이터와 승객 정보의 유출 우려, 그리고 철도 시스템의 안정성 위협 등이 제기 되었음.
  · 공급망의 취약점을 노린 공격으로는 2016년의 대우조선해양 해킹을 통한 국산 원자력추진잠수함 연구 내용과 같은 주요 군사 기술 자료

가 포함된 설계도 유출, 2019년 안랩 해킹 사건에서는 소프트웨어 개발 공급망의 취약점을 악용, 그리고 기타 여러 국내 SW 회사들의 해킹 피해, 국방부 그리고 군사 시스템 해킹, 2019년 POSCO 그리고 2020년 원전 해킹 시도가 있어 왔음

○ 국가 및 공공기관에 도입되는 IT 보안제품에 대해 현재는 국가정보원의 보안적합성 검증체계를 중심으로 공급망 사이버안보를 확보해 나가고 있음. 주로 HW 공급망안보 중심에서 차차 SW 공급망 보안을 위한 노력으로 향하고 있으나, 전자와 후자 더욱 보안 프레임워크를 구축하고, 이행을 위한 지원책을 마련해야 함

- 2022년 신정부 출범을 계기로 '제로트러스트 공급망 보안 포럼' 발족, 'SW 공급망 보안체계 구축을 위한 실증사업' 등 공급망 보안을 지향하는 정책이 추진되고 있음
- '정보통신망법', 'SW 진흥법', '정보통신기반보호법' 등에 개별법으로 산재하여 있으며, ICT 공급망 관련하여 적합한 보안 표준 및 관리체계를 규율하는 법령이 미비함
  · 세부적인 제도로는 '주요 정보통신기반시설 보호 제도', '보안 적합성 검증 제도', '공공기관 정보 시스템 구축·운영 지침' 등이 존재
- 일반적인 해킹이나 DDoS 등 사이버 침해 행위를 방지하려는 목적으로 제정된 법률이 분산된 형태로 존재하고 있을뿐 아니라, 내용도 일반적인 보안관리 조항들로 선언적 성격이 강함
- 국내 공급망 보안 R&D가 주로 HW 공급망 보안에 집중되어 왔으나, 최근에는 SW 공급망 보안을 위한 R&D도 다양해지고 있음
  · ETRI는 「시스템·디바이스의 HW 공급망 위협 대응 핵심기술 개발

('20~'24)」, 「임베디드 시스템 악성코드 탐지·복원을 위한 RISC-V 기반 보안 CPU 아키텍처 핵심기술 개발('21~'24)」을 추진 중. 고려대는 「고신뢰 온-디바이스 딥러닝 가속기 설계를 위한 물리채널 기반 취약점 검증 및 대응 기술 개발('21~'24)」을 진행 중. 그리고 SW 공급망 측면에서 「SW 공급망 보안을 위한 SBOM 자동생성 및 무결성 검증 기술 개발('22~'25)」을 추진 중.

- 지속적으로 HW뿐 아니라 SW 공급망 사이버보안 관련 민간 기업, 대학 및 연구기관들에의 지원과 협력이 요구됨
- 다른 한편, 동맹국이나 우방국들에서 제기되는 공급망 보안 이슈를 지속적으로 모니터링하고, 요구되는 보안 표준에 대해 대응 체계를 마련해야 함
  · 국내 보안 수준의 적절성을 추구하는 한편, 국제적 보안 시스템과 동조화(harmonization)는 아닐지라도 상호운용성(interoperability)을 도모해야 함

○ 한국은 2024년 5월 'SW 공급망 보안 강화 가이드라인' 1.0을 발표함

- 미국, 유럽 등 해외 주요국의 소프트웨어 구성요소 명세서(SBOM) 제출 의무화 등에 대응해 정부·공공 기관 및 기업들이 자체적인 소프트웨어 공급망 보안 관리역량을 갖출 수 있도록 지원하기 위해, 과학기술정보통신부·국가정보원·디지털플랫폼정부위원회는 민관 협력을 통해 만들어졌음. SW 품질을 높이고, 해외 무역장벽을 극복할 수 있기 위함임.
  · 판교 캠퍼스에서 테드스트베드를 운영 중이며, 공공기관 및 기업들이 SBOM을 쉽게 적용할 수 있도록 지원 중임. 2024년 하반기에 산·학·연 전문가들이 참여하는 범정부 합동TF를 구성하여 세부적인 정

부지원 방안, 제도화 추진방향 등에 대한 심도 있는 논의를 진행한 후 'SW 공급망 보안 로드맵'을 마련할 계획임

- 준비 없이 성급하게 도입할 경우, 기업들의 부담요인이 될 수 있기 때문에, SBOM 지원 적용책을 강화하는 한편, 소프트웨어 공급망 보안 저변 확대, 주요국의 제도화 동향과 국내 산업 성숙도를 검토할 수 있어야 함.
  · 이러한 다양한 측면을 고려하며 점진적으로 제도화를 준비하고 추진할 수 있는 체계적 조직 간 연계체계와 향후 과정을 볼 수 있는 HW·SW 공급망 보안 로드맵이 필요함

3. 국가 사이버 안보 대응 산업·기술 역량 강화

○ 2024년 국가 사이버안보 전략서에는 사이버안보 역량 강화와 인재 육성을 주요 목표로 설정하였음

- 한국의 소프트웨어 공급망보안 강화, 산업기술보호 정책, AI 및 신기술 관련 사이버 보안 정책, 사이버 보안 인증 제도 강화, 글로벌 기술협력 전략 등에서 모두 보안 산업의 역량 강화와 인재 육성의 필요를 언급하고 있음
- 이를 위해 사이버보안 R&D 투자 확대, 사이버보안 스타트업 지원, 사이버 보안 훈련 및 연습 확대, 민관 협력 및 국제협력 강화, 사이버 보안 전문가 양성을 위한 교육 프로그램 확대 그리고 대학 및 연구기관과 협력하여 관련 커리큘럼을 개발 중에 있음

○ 한국의 현장에서는 인재 부족을 호소함

- 사이버 교육과정을 운영하는 대학 감소
  · 보안 제품 및 서비스 개발을 위한 전문인력 양성 체계 미비. 특히 지역에 인력 공급방안이 요구됨
- 국가기반시설이 지능화됨에 따라 각 부문별 기반시설에 대한 이해와 사이버보안을 함께 이해할 수 있는 인력이 요구됨. 또한 스마트공장(IT+OT), 자율주행차(IT+자동차) 등 정보기술(IT)과 분야별 산업을 함께 이해하는 융합보안인력에 대한 수요도 증가
- 사이버전 확산, 사이버범죄 증가 등에 대응하여 민·군·경·원 협업을 통한 국방·치안·공공 분야 사이버 인력양성 강화 필요.

○ 2022년의 '사이버보안 전문인력 10만 명 육성 계획'을 윤석열 대통령이 발표함.

- 사이버안보 역량 강화를 위한 인력 확보 계획 제시함. 최정예 개발인력과 화이트해커 육성 체계를 통해 10만명(향후 5년 간 산업 수요에 대응하는 신규 인력공급(4만명), 재직자 역량 강화 교육(6만명)) 인재 양성 계획임. 사이버안보 기술을 전략산업으로 육성할 것임을 밝힘.
- 군 전문 분야 복무와 전역 후 취업과 창업을 연계하는 '사이버 탈피오트', 국가 비상상황에서 민관의 역량을 결집하기 위한 '사이버 예비군' 창설 등으로 사이버전 수행 역량을 강화할 것임을 밝혔음.
- 민간과 공공이 긴밀히 협력하는 사이버안보 대응체계를 공고히 하고, 민간과 공공 간 유기적인 정보공유 분석체계를 구축해 사이버위협을 효율적으로 예방·대응할 수 있도록 하고자 함
- 해당 계획이 선언된 판교 정보보호 클러스터는 실전형 사이버 훈련장,

사이버 교육장, 정보보호 스타트업 육성 공간, 사물인터넷(IoT) 테스트베드 등 인프라를 갖추고 있으며, 정보보호 스타트업 기업·인력의 협업과 성장을 지원하는 상징적인 장소임

○ 과기부의 '사이버 10만 인재 양성 방안'의 3대 중점과제가 포함됨

- 사이버보안 개발부터 대응까지 전주기 최정예인력 양성체계 구축
  · 융합보안대학원과 정보보호특성화대학 확대개편, '시큐리티 아카데미'를 도입하여 인재선발, 실무교육 취업 전과정을 주도, 기업내 사이버보안 인식 제고와 중소기업 보안인력 대상 교육지원 강화, '화이트햇 스쿨' 과정 통해 화이트해커 진입장벽을 낮춤
- 상시 육성 체계와 글로벌 연계기반 마련
  · '사이버훈련장' 확대, 지역교육센터와 지역정보보호 협의 구성해서 지역의 인재 양성과 지역 사이버산업 육성의 선순환 구조 마련
  · 개도국 인재 육성과 국내 기업의 해외 진출 지원하는 'K-사이버 글로벌 인력 네트워크(가)' 추진 그리고 한미 간 침해 대응기관 간 인력 교류
- 민관군 유기적 협력으로 사이버전 및 사이버 범죄에 대응
  · '사이버 탈피오트' 도입, '사이버 예비군' 창설, 국가 공공기관 정보보안담당자의 역량강화를 위해 지역대학과 연계, 금융·국방·전력 등 유관기관 합동팀이 나토(NATO) '락드 쉴즈', 미 '사이버 플래그' 등 국제 훈련에 참가, 침해대응기관 재직자 역량강화를 위한 나노 디그리 과정 추진 등이 포함됨
  · 육성뿐 아니라, 국가안보나 치안에 이들 인력을 활용하기 위한 법제도 마련이 필요함. 민간이 군사 작전 또는 치안 활동에 참여하기 위한 법적 근거가 필요함. 책무와 참여 범위에 대한 논의가 투명하게

만들어질 필요가 있음. 그리고 이러한 민관군 협력이 가져오는 효과에 대해 측정하고, 국내외 사회에 가져올 파장에 대해서도 예측할 필요가 있음

○ 한국은 사이버안보 인재 육성 방안을 목적에 맞게 분업화 및 체계화 필요가 있음

- 사회가 인터넷을 통한 초연결사회로 진화하며 사이버보안의 필요는 더 많아질 뿐 아니라 더 다양하게 될 것임. 이에 따라 각 산업이나 부문에서 요구되는 사이버보안 역량도 다양하게 요구될 것임
- 크게 세 부류의 인재로 나누고 정부 부처별로 집중할 수 있음. △공공, 치안, 국방을 위한 인재는 국정원, 경찰, 국방부가, △산업이나 회사를 위해서는 산자부와 민간이 함께, 그리고 △대중 교육, 정규 교육과 전문화 과정 그리고 연구 개발에는 과기부가 하는 방식으로 크게 세 부처가 나눌 수 있음. 그리고 위의 모든 인재 육성에는 대학이나 대학원 등의 교육계가 함께 함.
  · 그리고 각각의 부문에 맞는 인재 육성을 위한 교육 과정을 단계별로 그리고 영역별로 구분하여 체계화 시킬 필요가 있음
  · 예를 들어, 독일과 같은 경우, 자국의 강점인 제조 산업에 중점을 둔 사이버 보안 프레임워크와 기술들을 개발하는 데에 역점을 두고 있음
  · 한국도 강점인 산업을 중심으로 하는 사이버 보안 역량 강화에 집중할 수 있음
  · 한국의 지정학적 위치와 북한과의 특수한 관계에 기인한 사이버보안 인재 육성도 글로벌한 경쟁력을 가질 수 있음
- 과기부와 교육계가 표준화된 커리큘럼 제작을 통해, 사이버안보와 관

련한 용어들의 정의를 통일시켜서, 사회 내 여러 부문에서 활동하는 보안 담당자들 간에 원활한 협력이 이루어질 수 있게 해야 함. 그리고 인증 제도를 도입해서 표준화된 교육이 이루어질 수 있도록 해야 함.

- 이러한 분업은 미국과 중국에서의 인재 육성에 참여하는 정부 기관들이나 여러 프로그램 사례에서도 보임. 미국의 경우 상무부의 NIST, 국토안보부의 CISA, 국방부의 NSA가 민관협력을 통해 주도함.
  · NIST는 NICE(National Initiative for Cybersecurity Education) Framework, CISA는 Cybersecurity Talent Initiative, NSA는 National Centers of Academic Excellence in Cyber Defense(CAE-CD) 프로그램 운영

○ 사이버안보 인재의 해외 유출을 줄이고, 해외 인재를 유치할 인센티브를 마련할 필요가 있음

- 해외 인력 유치 또는 국제 인력 양성 협력을 위해, 적극적으로 국제회의나 워크숍을 유치할 필요가 있음. 한국의 지정학적 특수성에 기반한 기술에 특화된 것이면 더 좋음
  · 예를 들어, NIST는 여러 국제회의나 워크숍(RSA 컨퍼런스, 이스라엘 사이버 주간, 국제사이버 보안 챌린지, 미국-브라질 사이버보안 및 무역 워크숍, 글로벌 포럼 및 워크숍, 미국-싱가포르 사이버 대화)들을 개최함.
  · CISA에서는 Cyber Career Pathways Tool를 통해 국제파트너들에게 사이버 보안 직무 역할을 시각적으로 탐색하고 경로를 쉽게 찾을 수 있도록 지원함.
  · NSA의 국립 사이버 보안 우수 학술센터(NCAE-C) 프로그램은 학생과 교수진의 역량을 개발을 지원하며, 지역 사회 참여 및 전문성 개발을

강조하고 있음.

· 그 외에도 '사이버 보안 교육 다양성 이니셔티브' 그리고 'OnRamp II 프로그램'을 통해 STEM 분야 학생들에게 장학금이나 인턴십 기회를 제공하여 사이버 보안 연구 기회를 제공함.

· 중국의 경우도 위와 같은 미국의 체계와 교육 표준과 유사하거나 조금 못 미치는 것으로 파악됨.

- 미국으로의 인재 유출을 우려하는 캐나다는 혁신 이민 프로그램(Innovation Immigration Programs), 글로벌 인재 스트림(GTS)과 같은 프로그램을 운영 중

· 한국도 사이버보안 관련 인재 유치를 위한 이민 프로그램, 교육제도, 재정적 지원 등을 적극 고려할 필요가 있음

4. 사이버 안보 관련 기반 기술의 전략산업화

○ 2022년 신정부가 들어오며 사이버안보 분야의 전략산업화를 위한 노력이 꾸준히 진행되어 왔음

- 2022년 5월의 국정과제에 산업, 기술, 인재 경쟁력 제고가, 같은 해 9월 '대한민국 디지털 전략'에는 원천기술 확보, 4대(억제, 보호, 탐지, 대응) 방어기술 개발과 사이버전 대응역량 확보, 2022년 7월 '사이버보안 전문인력 10만 명 육성 계획'을 통해 우수 보안 스타트업 25개 창업 지원을 내놓았음. 10월에는 '국가전략기술 육성방안'이 나왔음

- 2023년 8월 과기부 장관에 의한 '2024년 국가연구개발사업 예산 배

분·조정 결과' 발표에 따르면, 사이버보안을 포함한 첨단바이오, 인공지능, 양자 등 7대 핵심 분야에 투자를 대폭 확대하는 등 혁신사업에 10조 원을 집중투자할 방침을 내놓았음

· 2023년 과학기술정보통신부 예산 중 정보보호 및 보안과 관련된 예산은 264억 원이며, 정보보호 인력양성에 163억 원, 정보보호 시스템 평가 및 인증기반 강화에 163억원, 정보보호 시스템 평가 및 인증기반 강화에 22억 원, 디지털 융합보안 기반-디지털 안전 선도모델 개발에 38억 원, 디지털융합보안 기반-양자기술 상용화 기반 조성에 41억원이 배정되었음

- 2023년 4월의 '전략적 사이버안보 협력 프레임워크'에서 보이는 바와 같이 사이버안보 분야의 전략산업화 노력이 국제협력 차원으로 확장되었음

○ 사이버안보 산업 부문의 인프라적 성격을 가지며, 지향하는 기술과 서비스에 따라 특성이 다름. 따라서 모든 부문에서 비즈니스를 전개하기보다, 다른 기업들과 차별화된 점을 내세우며, 자사의 가치를 높이고자 함

- 방화벽, DDoS, ID제어 등 기존 영역에서의 강점을 부각시키고자 하는 기업뿐 아니라 클라우드 보안, 제로트러스트, AI보안 등 최근의 기술을 기반으로 성장을 하고 있는 기업들도 존재함

· 예를 들어, Palo Alto Networks 기업은 방화벽 및 클라우드 기반 맞춤형 제품 개발에 집중하고 있으며, CrowdStrike는 엔드포인트 보안과 서비스, Cloudflare는 WAF, DDoS, CDN, DNS 등을 주 사업으로 하며, 시가총액 상위에 위치하는 5개 기업들은, 주로 네트워크, 클라우드, 엔드포인트 보안, 방화벽 등 최근 수요가 발생하는 영역에서

시장 경쟁력을 확보하고 있음

· 시가총액 상위 40개 기업의 대부분이 미국 기업이며, 이스라엘 4개 기업, 영국 2개, 일본, 독일, 프랑스, 인도도 각각 1개가 포함되어 있음

· 글로벌 사이버보안 유니콘 기업 수도 빠르게 증가추세이며 2019년 8개에서 2022년 59개로 증가함. 그리고 전통 빅테크를 중심으로 보안 기업들의 인수합병도 활발하게 일어나고 있음. 2023년 9월 Cisco의 Splunk 인수, 2022년 9월 구글 클라우드가 Mandiant 인수 등.

○ 국내 사이버보안 기업 중 가장 큰 매출을 보이는 기업은 안랩으로 2023년 매출이 2,298억원, 영업이익이 323억원, 이익률 14.1%를 기록함. 2023년 매출 1천억 원 이상인 국내 사이버보안 기업으로 시큐아이, 이글루코퍼레이션, 오픈베이스, 윈스 등이 있음

· 지란지교 시큐리티, 이스트소프트, 엑스게이트 등이 빠른 성장률을 보이고 있음

○ 현재 한국의 사이버 보안 시장은 상대적으로 작은 규모로 평가받고 있음

- 2023년 기준 한국의 사이버 보안 시장은 약 4.0조 원(약 31억 달러) 정도로 이는 글로벌 사이버 보안 시장의 약 1.9%를 차지하는 수준임. 반면, 미국의 사이버 보안 시장은 2023년 기준 약 94.8 조원(약 729억 달러)에 달하며, 전 세계 시장의 약 43.6%를 차지하고 있음. 한국의 사이버 보안 시장은 중국과 비교해도 매우 작은 편임
- 한국정보보호산업협회(KISIA)가 조사한 2023년 국내 정보보호산업 실태조사에 따르면 사이버 보안 분야에 종사하는 인력 중 상당수가 실무 경험이 부족하고, 최신 보안 기술에 대한 이해도가 낮은 것으로 평가

됨. 이는 글로벌 경쟁력을 저하시킬 수 있는 요인임

- 한국의 사이버 보안 기술력 또한 글로벌 시장에서 상대적으로 낮은 평가를 받고 있음. 한국의 사이버 보안 기업들은 주로 국내 시장에 집중하는 경향이 있으며, 글로벌 시장에서의 활동은 제한적임. 반면, 미국이나 이스라엘의 기업들은 초기부터 글로벌 시장을 겨냥하여 제품을 개발하고, 국제적인 네트워크를 통해 기술을 확산하고 있음.
  · 글로벌 경쟁력의 약화는 기술력 격차로 이어질 수 있음. 한국의 사이버 보안 기업들은 첨단 기술 개발에서도 다소 뒤처져 있다는 평가를 받고 있음. 특히 인공지능(AI), 머신러닝, 빅데이터 분석을 활용한 사이버 보안 솔루션 개발에서 미국과 이스라엘에 비해 경쟁력이 부족하다는 지적이 있음

○ 글로벌 시장으로의 확대를 위한 정부 지원 필요

- 국내 보안 시장만으로는 성장의 한계가 있기 때문에, 해외 시장 개척을 적극 정부가 지원해 나갈 필요가 있음
- 미국에서 글로벌 시장을 처음부터 노리고 진출한 이스라엘 기업 사례들이 좋은 모델이 될 수 있음
  · Check Point, CyberArk, Palo Alto Networks, Cybereason 등 다양한 이스라엘 사이버 보안 기업이 성공 사례로 있음
- 다양한 정부 기관에서 여러 프로그램을 통해, 자금, 기술 개발, 그리고 현지 기업이나 사람들과의 네트워크 형성을 지원할 수 있도록 해야 함
  · 예를 들어, 이스라엘은 8200 부대 출신 인력 활용, 벤처 캐피탈의 활용, 그리고 스타트업 팀의 구성에, 기술뿐 아니라, 제품 개발, 마케팅, 재무 관리 및 법률 지원 인력 포함

- 정부의 종합 패키지 지원 프로그램이 필요함. 그리고 벤처 캐피탈과 같은 자금력, 그리고 스타트업을 장려하는 국가 전체적 분위기가 요구됨. 창업 및 기술 혁신을 위한 기업가 정신 강조도 필요함

5. 신흥기술에 대한 사이버 위험 관리체계 확립

○ 2022년 윤석열 정부에서는 사이버 보안을 디지털전환 시대 필수기반 기술로 인식하고 12대 국가 전략기술로 지정하였으며, ▲데이터·AI 보안, ▲디지털취약점 분석·대응, ▲네트워크·클라우드 보안, ▲산업·융합 보안 기술을 중심으로 임무중심 전략로드맵을 수립하였음.

- 특히 SBOM 체계, 보안 특화 AI언어모델(LLM), 양자내성암호, 제로트러스트 등 글로벌 시장과의 보안 역량 동조화를 추진할 예정임

○ 한국정부는 신흥기술에 대한 사이버 위험 관리체계를 다각도로 준비 중임

- 2019년에 이어 2024년 국가 사이버안보 전략서에서는 신흥기술 관련 사이버 위협에 대한 대응을 강조하고 있음. 특히, 신흥기술의 유출과 주요 기반시설 운영에 신기술이 적용될 것으로 예상되는 바, 운영의 안정성과 효율성이 중요함
- 2022년 신정부 출범을 계기로 '제로트러스트 공급망 보안 포럼' 발족, 2024년 5월 'SW 공급망 보안 강화 가이드라인' 1.0을 발표를 통해, 국제 표준에 부합하는 보안체계를 구축하려고 함
- 2023년에 산자부에서 나온 '글로벌 기술협력 종합전략'에는, 초격차

기술, 차세대 산업원천 기술, 도전적 미래기술, 수요맞춤형 기술협력으로 구분하고 있으나, 이들 기술의 개발 및 사용에 동반하는 사이버 위협에 대해서는 언급이 없음.

○ 이전까지 공급망안보는 디지털 네트워크 장비 중심으로 국한되어 있었으나, 미국의 경우 최근 그 범위가 확장하며 첨단기술들로 확장하고 있음.

- 이는 곧 한국에게도 비슷한 수준의 공급망안보를 확보하기 위한, 정책, 표준, 또는 제도가 한국에게 요구됨을 의미함. 그러한 조치 없이는 미국과의 기술 협력은 어려울 것으로 예상됨
- 미 상무부에서 새로운 정책 도구들이 나오는데, '정보통신기술 및 서비스 프로그램(Information and Communications Technology and Services (ICTS) Program)'이 한 예임.
  · 해당 프로그램의 이행은 산업보안국(Bureau of Industry and Security)의 '정보통신기술 및 서비스 실(Office of Information and Communciations Technology and Services, OICTS)'에서 담당하고 있으며, OICTS의 임무는 미국의 특정 ICTS 거래가 미국에 국가안보 위험을 가하고 있는지 여부를 조사하는 것임
- OICTS는 기술 우선순위(2024 Technology Prioritization) 표를 만들어 제시하고 있는데, 이를 통해 향후 국가가 정책이나 투자를 통해 우선적으로 개입할 방향이 보이고, 해당 기술들의 공급망 안보를 확보하기 위한 수단들과 수출통제를 병행해 나갈 것임
  · 우선순위가 높은 기술들은 주로 국방, 사이버안보, 경제성장에 중요한 것들이기도 함. 트랙 I은 국방과 통신보안, 트랙 II는 국방과 상업적 응용에 필수적인 고급기술, 트랙 III는 보안 및 상업에 큰 영향을

미칠 신흥기술들을 포함하고 있음

〈표 4-1〉 OICTS는 기술 우선순위(2024 Technology Prioritization)

우선순위	트랙 I	트랙 II	트랙 III
높음	· 위성 접속 지점 · 모바일 네트워크 하드웨어	· 고급 및 네트워크 센서 · 에너지 생성 및 저장 · 자율 시스템 및 로봇공학 · 반도체 및 마이크로프로세서	· 서비스형 인프라 · 고급 클라우드 서비스 · 연결된 차량
중간	· 네트워크 보안 및 운영	· 인공지능 · 우주 기술 및 시스템 · 고급 컴퓨팅 · 데이터 프라이버시 및 사이버 보안	
낮음		· 위치, 내비게이션 및 타이밍, · 양자 정보 기술	

○ 한국의 사이버 보안 기업들은 첨단 기술과 관련한 사이버보안 기술에서 다소 뒤처져 있다는 평가를 받고 있음.

- 특히 인공지능(AI), 머신러닝, 빅데이터 분석을 활용한 사이버 보안 솔루션 개발에서 미국과 이스라엘에 비해 경쟁력이 부족함. 특히 인공지능(AI), 머신러닝, 빅데이터 분석을 활용한 사이버 보안 솔루션 개발에서 경쟁력이 부족함
- 한국 정부는 신흥기술이 포함될 주요 인프라뿐 아니라 더 넓은 범위의 조직 및 기관들을 포함한 사이버안보 프레임워크(미국 NIST 사이버안보 프레임워크 2.0)를 만들어 표준을 세우고, 위기 관리 거버넌스를 만들며, 식별, 보호, 탐지, 대응, 회복 그리고 거버넌스를 위한 기능을 강화하도록 해 나가야 함

· 그리고 디지털 자산의 목록을 만들고 유지하며, 정보를 위험과 중요도에 따라 분류해야 하며, 매년 심사와 모니터링을 할 수 있도록 해야 함

· 한국은 CSK 2024에서 '국가망 보안정책 개선 로드맵', '전 공공분야 국제표준암호 AES 허용 계획'을 발표함

- 정부는 인공지능, 양자 컴퓨팅, 양자내성 암호화 등 신흥 기술 연구에 대한 투자를 확대해야 함

○ 첨단 기술과 관련한 사이버보안 법을 제정할 필요가 있음. 그러나 첨단 기술의 발전 및 변화 속도가 매우 빠르기 때문에 필요하면, 미국의 대통령 행정명령과 같은 방안으로 발 빠르게 대처하는 방법을 적극 구사할 필요가 있음

- 한국에는 행정규칙과 법규명령이 있으나 대통령 명령(order)은 아님, '대통령령', '긴급명령권'은 법률을 집행하기 위한 것이기에 행정명령보다 범위가 매우 제한적임. 박정희 정권 시기 '긴급조치'는 민주화 이후 위헌으로 결정됨. '기본계획', '시행계획'을 통해 보완 가능.

- 미국은 '양자컴퓨팅 사이버보안 준비법(Quantum Computing Cybersecurity Preparedness Act)'이 2022년 하원에서 통과됨

· 양자컴퓨터에 의해 해독될 수 있는 정보기술 시스템의 목록을 작성 및 유지하고 있으며, 양자내성 암호로 전환하기 위한 지침을 준비 시작함. 새로운 표준이나 전환을 위한 일정이 나오게 되면 규제로서 작동하게 되는데. NIST가 2024년 8월 세 가지 양자내성 암호 표준을 승인함.

· 민간도 이에 상응하는 보안 역량을 신장해야 함. 법은 연방 기관만을 대상으로 하지만, 정부 계약 자격을 유지하고 평판을 높이기 위해 민

간 부문도 이러한 지침을 따를 것으로 예상됨

· 한국에게도 필요시, 신속하고 안전하게 암호 알고리즘을 전환할 수 있는 능력, 즉 "암호학적 민첩성(cryptographic agility)"이 요구됨. 암호학적 민첩성은 빠르게 변화하는 기술 환경과 새로운 보안 위협에 대응하기 위한 중요한 전략임

- 미국은 관리예산처에서 연방 기관들의 AI 사용에 관한 지침을 발표, 상무부는 위험 관리를 위한 가이드라인과 도구를 개발 중, 보건복지부도 의료분야 AI 사용 전략 계획 수립 예정, 국토안보부도 AI 관련 주요 기반시설 보호를 위한 국제협력 전략을 수립 중임

- AI, 퀀텀, 우주 분야와 같은 신흥 기술에서의 사이버 위험 관리 방안은 다음을 들 수 있음

· △보안 중심설계(Security by Design)(취약한 네트워크 분리 및 원격 연결 제한 등), △다층방어(Defense in Depth)(데이터 암호화 및 OT/IT 네트워크 분리 그리고 산업 표준 및 프레임워크(NIST, IEC 62443, ISO 27001 등 적용), △상황 인식 강화(지속적인 위협 환경 모니터링 및 분석 그리고 실시간 운영 경보 시스템 구축), △기본적 사이버 위생 준수, △정보 공유(산업 내 및 정부와의 협력 강화 및 위협 인텔리전스 서비스 활용), △사고 대응 및 준비태세(신속한 대응을 위한 모니터링 도구 활용, 인터넷 분리 운영 능력 확보, 그리고 자동화된 취약점 평가 도구 사용), △교육 및 복원력 강화, △IT/OT 융합 보안 전략 수립, 신기술 활용(AI 및 머신러닝을 활용한 보안 강화, 자동화 및 가시성 솔루션 구현), △지속적인 위험 평가 및 관리(IT/OT 자산의 취약점 파악 및 위험 평가 정기적 실시 그리고 동적이고 적응적인 보안 접근 방식 채택)을 들 수 있음.

제5장

사이버 군사전략과 동맹협력

윤 대 엽 | 대전대학교 군사학과 교수

1. 한미 사이버 동맹협력의 심화
2. 북핵위협 대응 사이버 군사전략
3. 사이버 상호운용성과 합동성 증진
4. 사이버 집단안보체제 구축
5. 국방 사이버 전문인력 양성

제5장

사이버 군사전략과 동맹협력

윤 대 엽 | 대전대학교 군사학과 교수

배경과 구성

- 제5장은 전통적 한미 상호방위조약의 대상을 사이버 공간으로 확장한 2023년 4월 '한미 전략적 사이버 안보협력 프레임워크(SCCF)' 이후 한미 동맹협력의 과제를 (1) 사이버 상호운용성, (2) 북핵대응을 위한 비대칭 사이버 우위전략, (3) 사이버 집단안보 등 세 가지 영역에서 검토
- 첫째, 사이버 위협에 대응하는 한미동맹의 사이버 상호운용성(interoperability)의 심화를 위한 전략적, 작전적 기술적 과제를 세부적으로 검토
- 둘째, 북한의 비대칭 위협 수단이자, 북핵위협을 억지, 방어하는 사이버 우위를 위한 사이버 군사전략의 과제를 '디지털 로우-하이 믹스' 전략 개념을 통해 검토
- 셋째, 디지털 기기, 네트워크, 플랫폼을 넘어 인공지능, 빅데이터, 클라우드로 확장되고 있는 국방체계의 디지털 전환에 수반되는 사이버 위협대응을 위한 사이버 집단안보(cyber collective security)의 과제 검토

- 제5장의 구성은 아래와 같은 다섯 가지 항목을 중심으로 함

  1. 한미 사이버 동맹협력의 심화
  2. 북핵위협 대응 사이버 군사전략
  3. 사이버 상호운용성과 합동성 증진
  4. 사이버 집단안보체제 구축
  5. 국방 사이버 전문인력 양성

1. 한미 사이버 동맹협력의 심화

○ 2023년 4월 한미동맹 70주년을 계기로 한미 정상은 '한미 전략적 사이버안보 협력 프레임워크(Strategic Cybersecurity Cooperation Framework, SCCF)'를 발표하고 사이버 공간을 한미상호방위조약의 영역에 포함함

- SCCF는 1) 사이버안보를 국가정책 및 동맹협력의 영역에 포함하고, 2) 모든 범위의 사이버위협을 억지, 거부, 방어, 대응하기 위해, 3) 사이버안보, 기술, 정책, 전략, 훈련 등의 협력을 증진하며 (7가지 항목), 4) 한국의 국정원, KISA, NCSC, 국가사이버위기관리단 및 미국의 CISA 등의 관련기관 협력을 명시
- SCCF는 '동맹이 사이버 공간에 적용된다는 것을 인식하고 한미는 상호방위조약이 어떻게 적용될지와 어떤 상황에서 적용될 것인지에 대한 논의 시작'을 명시
- 특히, 양국 정상은 전통적인 육해공 국방의 안보동맹이 사이버 안보 분야로 확장되는 것을 '사이버 우산(Cyber Umbrella)' 개념으로 정의함 (대

통령실 23/04/27)

○ 한미 국방부는 2013년 10월 제45차 SCM에서 국방사이버정책실무협의회(Cyber Cooperation Working Group, CCWG) 구성에 합의한 이후 사이버 안보협력을 한미안보동맹의 핵심의제로 진전시키고 있음(김상배 2023, 14)

- 국장급 협의체인 CCWG는 사이버 위협에 대비한 대응 능력 향상을 위해 정보공유 및 사이버 정책, 전략, 교리, 인력, 훈련 관련 협력 강화 추진
- 2023년 5월 제8차 CCWG에서는 1) 사이버위협 및 도발양상, 해커조직에 대한 정보공유, 2) 다국적군 연합사이버방어훈련, 3) 사이버위협 준비태세 및 연합작전능력 강화를 위한 훈련준비 등 논의 (국방부 보도자료 2023)
- 특히, 한국과 미국의 사이버작전사령부는 2024년 1월 15-26일 한국 사이버작전사령부 훈련장에서 최초의 사이버 동맹 훈련을 개최함
- 뿐만 아니라 한미 국방부는 2021년부터 '한미 ICT협력위원회'를 신설하고 1) 사이버 보안 공동지침, 2) 5G EMD 국방정보통신기술 협력, 3) 상호운용성과 연합전력 기반 지휘통제 및 정보교육체계 구축방안에 대한 협력을 확대
- 2024년 6월 다영역작전(MDO) 차원에서 실시된 '프리덤 에지' 훈련은 육해공 및 우주, 사이버, 전자기 영역에 대한 한미일의 연합훈련 시행

○ 미 국방부는 2010년대 들어 사이버 전략에서 동맹협력의 중요성을 기술하고 있으며, '2023 사이버 전략(2023 Cyber Strategy)'도 목표, 영역을 구체적으로 명시

- 2018년 국방 사이버 전략은 1) 동맹국과 파트너의 역량 강화, 2) 파트너

의 기술, 자원, 역량 및 관점을 활용하여 미국의 능력 보완, 3) 사이버 공간 운영의 효율성 증대 및 집단적 사이버 안보(collective cyber security)를 강화하고, 4) 사이버 공간에서 책임있는 국가의 행동규범 강화 등 4개 동맹협력 목적을 제시함 (DoD 2018, 5)

- 2023년 국방 사이버전략은 1) 사이버 공간에서 동맹국, 파트너의 역량이 정보공유, 상호운용성 및 집단안보에 기여하지만, 2) 상호의존성이 미국을 공격하는 사이버 행위자들의 목표가 될 수 있다는 점에서 리스크를 수반한다고 기술(DoD 2023, 11).
- 따라서, 전략적, 작전적, 전술적 수준에서 동맹국, 파트너와의 협력 강화 추진
- 특히 규범과 질서형성 등의 협력와 함께, 1) 네트워크의 취약점 식별, 2) TTP와 멀웨어 방어훈련과 사이버 회복탄력성 강화, 3) 인력개발 및 운영협력 등 '헌트 포워드 작전(Hunt Forward operations)'의 지속 목표를 명시함

〈표 5-1〉 미 국방부 사이버 전략목표 2018-2023

2018 DoD Cyber Strategy	2023 DoD Cyber Strtegy
· 더욱 치명적인 합동성 건설	· 국가방어
· 사이버 공간에서 억지와 경쟁	· 전투준비와 전쟁에서의 승리
· 동맹 강화 및 신 파트너십 협력	· 동맹 및 파트너와 사이버 도메인 보호
· 국방부의 개혁	· 사이버 공간에서 지속적인 이익구축

○ 미중경쟁이 본격화된 이후 제3차 상쇄전략의 맥락에서 추진되고 있는 미국의 군사혁신은 모두 동맹협력의 중요성을 강조하고 있음

- 미국은 미중경쟁이 본격화된 2017년 이후 국방체계의 디지털 전환, 인

공지능 지원 국방체계의 기반구축을 위해 인공지능전략(2018), 디지털 엔지니어링 전략(2018), 클라우드전략(2018), 디지털현재화전략(2019), 데이터전략(2020), 국방사이버전략(2022)을 발표하고 2023년 인공지능, 빅데이터, 클라우드 전략을 통합한 데이터, 분석, 인공지능 전략(2023)을 발표

- 2018년 발표된 인공지능 전략은 인공지능의 군사적 활용이 미국의 군사적 우위는 물론 동맹국, 협력국의 방어기반으로서 효율성, 경제성 및 속도를 향상한다고 명시
- 디지털 엔지니어링 전략은 무기체계의 기획, 소요, 연구, 개발, 생산, 운용 및 성능개량 등 총수명주기체계 전반의 모듈화, 모델링 기반으로서 디지털 엔지니어링의 혁신이 국방부, 민간부문 뿐만 아니라 동맹국, 협력국의 포괄적인 협력영역 명시
- 인공지능 기반 지휘결심의 기반으로서 정보네트워크를 구축하는 클라우드전략(DoD 2018c)은 데이터 기반 결정을 위해 동맹국과 데이터 공유 및 연합작전 능력의 향상기반으로서 국방클라우크를 정의함
- 디지털 기반 광범위한 상호운용성의 과제를 세부적으로 규정하고 있는 디지털 현대화전략(DoD 2019)은 동맹국, 협력국과의 책임있는 정보공유 기반으로서 ICAM(End to End Identity, Credential, and Access Management) 구축 명시
- 2020년 처음 발표된 데이터전략(DoD 2020)은 데이터 및 데이터 공유 기반이 동맹국, 협력국과의 연합자전의 전략적 자산임을 명시함
- 2022년 국방전략은 개방적 혁신기반을 가진 동맹국, 협력국과의 네트워크가 미국의 경쟁우위 요인이며, 2023년 발표된 '데이터, 분석, 인공지능전략'(DoD 2023)은 동맹국, 협력국과 데이터, 분석, 인공지능 관련

전략, 제도, 기술의 상호운용성을 공유하는 목표가 명시되어 있음

〈표 5-2〉 미국의 주요 안보전략서와 동맹협력

목표	세부추진과제
인공지능전략 (2018)	· 동맹국, 협력국의 방어기반으로서 인공지능 활용 · 효율성, 경제성, 속도의 향상
DE전략 (2018)	· 디지털 엔지니어링의 혁신을 위해 국방부, 민간부문, 동맹국, 협력국의 포괄적인 협력 필요
클라우드전략 (2018)	· 데이터 기반 결정을 위해 동맹국과 데이터 공유 및 연합작전 능력 향상
디지털현대화전략 (2019)	· 동맹국, 협력국과의 책임있는 정보공유를 위해 ICAM(아이덴티티, 자격인증, 엑세스 관리) 기반 구축 · 디지털 기반 동맹 상호운용성
데이터전략 (2020)	· 데이터는 동맹국, 협력국과 연합작전의 전략적 자산
국방사이버전략 (2022)	· 동맹 및 협력국과 사이버 도메인 보호 · 사이버 공간에서 지속적인 이익 추구
국가방위전략 (2022)	· 개방적 사회, 혁신기반 및 동맹국, 협력국 네트워크는 경쟁우위기반
데이터, 분석, 인공지능 전략 (2023)	· 공동의 도전에 협력, 공유된 이익 증진, 민주적 규범과 가치 보호를 위한 동맹국과의 상호운용성 · 동맹국, 협력국과 데이터, 분석, 인공지능 관련 전략, 제도, 기술의 상호운용성 공유 · 학계, 산업계, 동맹국 및 협력국과 데이터 관리, 책임있는 AI, AI 준비태세 협력

○ 한미동맹이 사이버 동맹(cyber alliance)로 확장, 실행하기 위해서는 1) 사이버 위협의 우선순위와 목표에 대한 전략적 상호운용성, 2) 사이버 억지, 방어, 공격의 작전적 상호운용성 뿐만 아니라, 3) 디지털 기기, 데이터의 기밀성, 가용성, 통합성 등 제도적 상호운용성, 4) 기술적 상호운용성

의 과제가 단계별로 추진될 필요가 있음

- 국방사이버 전략, 작전, 전술은 보안(security), 방어 뿐만 아니라 능동적 방어(active defense), 공세적 방어(offensive defense), 선제적 방어(defend forward) 및 헌트 포워드(hunt forward) 등 공격목적의 독트린, 기술과 협력을 포함한다는 점에서 사회차원의 사이버 안보전략과 차별성이 있음
- 미군은 군사적 사이버 작전을 1) 네트워크 내부 작전(Network Operations), 2) 방어적 사이버작전(DCO), 공세적 사이버 작전(OCO)으로 구분
- DCO는 내부방어조치(internal Defensive Measures)와 대응조치(Response Actions)로 개념화되어 있지만, 그린 사이버공간을 제외하면 회색, 적색 사이버 공간(gray and red cyberspace)의 방어적 작전과 공세적 작전의 명확한 경계선이 없음
- 특히, 상시적인, 공격우위의 사이버 위협이 고도화되면서 선제적 방어, 헌트 포워드 등 공세적 전략에 따라 능력, 수단(디지털 하드웨어와 소프트웨어, 부대) 개편

〈표 5-3〉 미군 사이버작전(CO) 개념

영역	개념	미국 작전교리(FM)
NO	사이버 보안	· 네트워크, 장치 등의 구축 능력 보존, 보호 · 사이버 네트워크 내부 – Blue Cyberspace
DCO	농동적 방어	· 네트워크의 취약점을 선제적으로 찾아 위험을 줄이고, 사이버 공격을 실시간으로 발견, 추적, 분석, 대응할 수 있는 역량
	공세적 방어	· Cyber Exploitation (사이버 이용) – 정보감시 · 회색, 적색 사이버 공간에서 미래 군사작전을 준비하기 위해 정보 수집, 감시 등의 활동으로, 네트워크, 시스템 및 군사적 가치에 대한 엑세스 확보, 사이버 지속(Cyber Persistence)

영역	개념	미국 작전교리(FM)
OCO	선제적 방어	· 선제적 방어(Defense Forward)는 시스템, 네트워크에 접근하여 방해, 저하, 파괴하여 적대적 사이버 공격에 비용 부과
	헌트 포워드	· 명확하지 않음, 안전, 방어, 공세작전 포괄, 초국경성 · 적대국이 사이버 공격에 활용할 목적으로 미리 자국, 동맹국의 네트워크 시스템에 침투, 심어놓은 악성 프로그램을 차단하거나 걷어내는 작전 (신소현 2022, 5)

- NO, DCO 차원의 한미 사이버 안보협력을 공세적 사이버 작전으로 확대하고, 장기적으로 통합적 상호운용성을 위해 단계적 안보협력 과제 추진
  - 사이버 동맹은 전통적 동맹을 사이버 영역으로 확대한 미국 의존 확장억지(extended deterrence)가 아니라 미군을 포함하여 모든 국가가 추진하는 다차원통합작전을 지원하는 통합적 억지력(integrated deterrence)을 강화하는 것임(김상배 2024)
  - 통합적 상호운용성은 네트워크 보안, 시스템 보호 차원의 사이버 안보 전략을 디지털 기술, 네트워크, 시스템(C4ISR), 데이터, 클라우드로 확장하고 궁극적으로 인공지능 지원 유무인복합체계 및 자율무기체계의 상호운용성을 목표로 함
  - 이를 위해 NO, DCO 전략, 교리, 정책, 훈련을 공유하는 한편, OCO 영역에서의 협력 및 육해공, 우주, 및 비국방망(non-Defense information Network), 초국경적인 협력을 포함하는 통합적 상호운용성의 협력 필요 (세부적인 논의는 3절 참조)

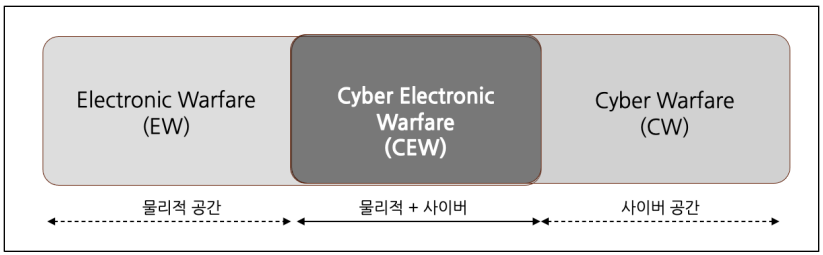
2. 북핵 대응 사이버 군사전략

○ 한미 사이버 동맹은 사이버 공간에 대한 북한의 비대칭 위협에 대응하고, 북핵위협을 억지, 방어하는 한미동맹의 비대칭 우위전략의 수단이 될 수 있음

○ 디지털 전환에 따라 디지털 기기, 네트워크가 혼잡해지고(contested), 사이버 공간의 취약성을 활용하는 군비경쟁이 심화되면서 사이버-전자기 스팩트럼(electromagnetic spectrum)을 통합하는 전략적, 작전적 변화가 진행되고 있음

- 무기체계, 지휘통신(C5ISR)은 물론 장기적으로 전장사물인터넷(IoBT), 클라우드에 기반하는 자율/반자율 무기체계 등 군사체계의 디지털 전환에 따라 사이버 공간은 전자기 스팩트럼을 이용하여 무선 네트워크 공간, 기기, 능력 교란, 파괴하는 전자기작전(Electonic warfare)과 통합되고 있음

〈그림 5-1〉 사이버·전자기 영역의 통합과 작전목표(아래)



구분	사이버전	전자기전	사이버전자기전
목표	사이버 수단	물리적 표적	물리적+사이버
공격	소프트웨어	전자기스팩트럼	사이버+멀웨어
영향	사이버, 데이터	시스템 파괴	시스템+물리적

- 미국은 사이버·전자기 작전교리를 통합하고(2021), 사이버작전사령부는 물론 대대급 I2CEWS(Intelligence, Information,Cyber Warfare, Electromagnetic Warfare and Space) 기능을 통합하여 항법위성 메시지 탐지/분석, 허위/기만 메시지 생성 및 송출 등 사이버 네트워크 체계의 물리적/비물리적 보호, 방어, 공세를 위한 교리를 발전시키고 있음
- 미국, 유럽아프리카사령부(독일)과 인태사령부(하와이)에 배치된 다영영 특임여단(MDTF)은 합동전영역작전(JADO)을 위해 I2CEWS대대에 장거리타격(Strategic Fires), 방공대대(Air defense)를 통합한 부대임

○ 사이버 공간의 위협을 사이버 수단으로 대응하는 전통적 사이버 군사전략이 사이버-전자기파의 통합적인 전략으로 전환되는 1) 물리적/비물리적 공간의 차이를 소멸시키고, 2) 네트워크 망 내부뿐만 아니라 디지털 기기, 플랫폼, 데이터 등 디지털 체계의 체계화로 통합되는 기술적 변화 때문임

- 전통적으로 사이버 작전은 1) 사이버 공격에 사이버 수단을 동원하여 대응하는 사이버-사이버 작전(Cyber-Cyber Opearation)의 개념, 능력, 수단에 집중
- 2) 사이버·전자기 영역이 통합되면서 사이버 공격(능력)을 군사적 수단으로 마비, 파괴하는 사이버-군사적 작전(C-M Operation) 개념으로 확장
- 3) 발사왼편전략(Left-of-Launch)과 같이 군사적 위협을 사이버 수단을

통해 억지, 방어, 공격하는 군사적-사이버 작전(M-C Operation)개념도 발전하고 있음

- 사이버 동맹협력의 심화를 위해서는 전통적 사이버 작전(C-C operation)은 물론 M-C 작전, C-M 작전도 전략적, 통합적 시각에서 발전시킬 필요가 있음
- C-M 작전의 대상은 (1) 사이버 부대 및 관련시설, (2) 통신, 데이터, 지휘통신 스테이션 및, (3) 전력, 지원시설 등이 포함할 수 있음

〈그림 5-2〉 사이버·전자기 작전영역

		공격 수단	
		사이버 공격	군사적 공격
대응수단	사이버 수단	(1) C-C Operation	(3) M-C Operation
	군사적 수단	(2) C-M Opeation	(4) M-M Deterrence

○ 사이버·전자기 작전영역의 확장, 통합에 따라 비대칭 사이버 위협(asymmetric cyber threat)에 대응하는 통합적 전략목표와 능력, 수단을 구축할 필요가 있음

- 디지털 전환에 비례하여 디지털 리스크 및 취약성 증가
- 비대칭 우위를 위한 군사혁신 경쟁이 심화되고 있는 가운데 사이버·전자기 영역은 기술적, 전략적 비대칭 공격수단이 될 수 있음

〈그림 5-3〉 비대칭 사이버 작전영역

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">사이버 공격대상</td></tr>
<tr><td>대군사목표</td><td>대가치목표</td></tr>
<tr><td rowspan="2">사이버
작전목표</td><td>간접적</td><td rowspan="2">대칭적 군사전략</td><td rowspan="2">비대칭 군사전략</td></tr>
<tr><td>직접적</td></tr>
</table>

- 탈냉전 이후 대칭적 군비경쟁이 제한되었던 북한은 핵·미사일, 장사정포, 특수전, 생화학무기, 사이버 등 비대칭 전력을 강화해 온 가운데, 최근 무인기 침투, 오물풍선 사례가 대변하듯 비대칭-비전통 수단을 동원한 도발 증가
- 사이버·전자기전의 목표는 대군사(counterforce) 목표가 아닌 대가치(countervalue)를 대상으로 하며 특히, 인공지능의 무기화는 비대칭 살상무기가 아니라 정보심리전, 인지전 등 비대칭 비살상무기(non-lethal weapons) 위협이 증가함
- 핵무장한 약소국일 뿐인 북한은 핵 강압을 수단으로 디지털 범죄, 사이버 테러, 정보심리전, 디지털 인지전 등 비전통-비대칭 수단을 연계한 사이버 공격 증가
- 한편, 남북간의 군사적, 사회적 디지털 기반의 비대칭을 고려할 때 북한의 비대칭 사이버 위협에 대응하는 포괄적, 통합적 우위의 전력 수단이 될 수 있음

3. 사이버 상호운용성과 합동성 증진

○ 한미 사이버 동맹이 전통적 확장억지가 아닌 통합적 억지력의 기반이 되기 위해서는 1) 전략적, 2) 작전적, 3) 제도적, 4) 기술적 상호운용성의 협력심화 필요

〈표 5-4〉 통합적 상호운용성과 사이버 동맹협력

구분	사이버 동맹협력의 세부과제(예시)
전략적 상호운용성	· 사이버 위협 및 우선순위와 목표
작전적 상호운용성	· 사이버 억지, 방어, 공격 등 사이버 군사전략 · 사이버 위협 정보공유 (risk information sharing) · 사이버 취약성 평가 및 훈련
제도적 상호운용성	· 사이버 보안정책 및 절차 · 디지털 기기, 데이터 보호의 기밀성, 가용성 협력
기술적 상호운용성	· 군사적 사이버 수단(weapons) 개발, 운용 · 제3자 및 공급망 리스크 · 다자 사이버 신뢰구축 및 표준협력

- 한미 SCCF합의는 사이버 동맹협력을 위한 출발점으로 사이버 작전의 상호운용성을 위해 NO, DCO 전략, 교리, 수단, 훈련을 OCO 영역으로 확장추진
- 이를 위해서는 사이버 보안정책 및 절차, 디지털 기기, 데이터의 기밀성, 가용성 등에 대한 제도적인 절차와 기준에 대한 제도적 상호운용성이 검토될 필요가 있음
- 기술적 상호운용성은 디지털 기술, 디지털 기기, 사이버 무기의 개발, 운용, 훈련에 있어서 협력은 물론 제3자의 공급망 리스크를 포괄하는

개념

- 육해공군은 물론 우주 및 비국방망(Non-DoD Information Network) 및 초국경적인 국제협력을 포함하는 전략을 공유하는 통합적 상호운용성은 네트워크와 시스템 차원의 사이버 안보전략을 디지털 기기, 네트워크, 시스템(C5ISR), 데이터, 클라우드 등 디지털 플랫폼으로 확장하여 통합적 안보전략 개념임

○ 첫째, 사이버 상호운용성을 위해서는 사이버·전자기 영역의 통합 및 비대칭 사이버 위협에 기반하여 통합적, 다차원 전략목표가 수립되어야 함

- 사이버 우세는 수세적, 방어적 목적에 그치지 않고, 공세적 능력에 기반하는 억지력으로 활용될 수 있으며, 이를 위해서는 C-C 작전 이외, M-C 작전, C-M 작전을 사이버정보, 심리, 인지전 등 사이버 비대칭 전략과 연계하는 통합적 사이버 작전전략이 수립 필요
- 북핵위협 대응에 특화되어 있는 한국군의 주도로 보안, 방어적 사이버 작전(DCO), 공세적 사이버 작전능력의 혁신을 우선하되, 한미동맹의 상호운용성 영역을 현재 방어적 사이버작전에서 공세적 사이버 작전으로 확대하고, 사이버·전자기 영역의 통합적 상호운용성으로 확대 추진

○ 둘째, 통합적 상호운용성의 기반으로 디지털 상호운용성 개념

- 디지털 상호운용성은 디지털 기기, 체계의 개념, 소요, 설계, 연구개발 및 운용, 폐기 등 총수명주기체계 상에서 기술, 운용, 보안의 상호운용성을 체계화하는 것임
- 인공지능, 빅데이터, 클라우드 기반 디지털 전환이 가속화되면서 기기, 체계, 네트워크는 물론 중장기적으로 데이터와 클라우드 등 시스템의

시스템으로 통합이 진전되고 있음

- 상호연결된 방대한 디지털 자산과 빅데이터, 클라우드 기반이 사이버 군사전략의 수단이자 기반이라는 점에서 디지털 자산의 설계, 생산은 물론, 운용을 위한 네트워크, 데이터의 활용 등 디지털 기반의 모든 단계에서 기술, 체계, 보안의 상호운용성이 설계, 운용되어야 함

○ 기술, 시간, 자원이 소요되는 국방부문의 디지털 전환과 디지털 상호운용성의 통합에 있어 전략-자원 합리적인 디지털 로우하이 믹스 전략을 추진할 필요 있음

〈그림 5-4〉 디지털 로우-하이 믹스전략

		네트워크 통합 수준	
		높음	낮음
디지털 전환 수준	높음	DIGITAL HIGH	DIGITAL MIDDLE
	낮음	DIGITAL MIDDLE	DIGITAL LOW

- 보안성, 폐쇄성을 특징으로 하는 국방 네트워크의 특징을 고려할 때, 통합적 운용이 우선되어야하는 전략적, 기술적 우선순위에 따라 '디지털 로우-하이 믹스(digital low-high mix)' 개념에 따라 디지털 상호운용성의 단계적이 협력 검토
- 디지털 하이-로우 믹스는 1) 디지털 전환수준과 2) 네트워크 통합수준에 따라 세가지 영역으로 구분할 수 있음
- 예를 들어, 인공지능 기반 유무인 복합체계의 경우 클라우드 기반 네트워크에 통합된 체계와 통합되지 못한 체계의 전략, 성능, 활용에 근본적인 차별성이 있음

- 하이급 디지털 기반 사이버 상호운용성은 물론 로우급 사이버 위협에 대한 동맹협력 등 강한 고리와 약한 고리의 동시적, 일체화된 협력이 포괄적으로 검토되어야 함
- 한미동맹의 상호운용성을 위해 연구개발, 공급망, 장비품에 대한 생산, 정비 등의 협력이 필요하며, 일례로 미일은 2023년 미일방위회담에서 1) 연구개발의 신속화, 2) 방위장비 및 부품의 공급망 협력, 3) 미일 공동장비품의 생산, 유지, 정비에 대한 기술협력에 합의하고, 2024년 4월 미일 정상회담에서 지휘, 작전은 물론 기술적 상호운용성의 강화목표 합의한 바 있음

○ 셋째, 통합적 상호운용성을 선도하는 부대개편이 수반되어야 함
- 인공지능, 빅데이터, 클라우드 기반 디지털 전환이 가속화되면서 기기, 체계, 네트워크는 물론 중장기적으로 데이터와 클라우드 등 시스템의 시스템으로 통합이 진전되고 있음
- 미군은 2018년 5월에 통합군으로 격상된 사이버군이 사이버 공간에서의 작전을 총괄하고, 1) 국방부의 정보 환경을 운용·방어하는 '사이버 방호부대'(68팀), 2) 국가 수준의 위협으로부터 미국의 방위를 지원하는 '사이버 국가 임무부대'(13팀), 3) 통합군이 실시하는 작전을 싸이 바면에서 지원하는 '사이버 전투 임무 부대'(27팀) 등 133개 '사이버 임무 부대' 25개의 지원팀 등 6,200명의 병력 운영
- 최근 우주작전을 지원하는 14개의 우주작전팀의 신설을 결정한 바 있음
- 사령부 및 작전적, 전술적 차원의 사이버 작전을 수행하는 부대는 전략, 전술, 기술적 상호운용성을 심화시키는 실질적인 기능 수행

4. 사이버 집단안보(Cyber Collective Security) 구축

- 개방성과 상호운용성은 디지털 기반 군사체계의 효과성은 물론 사이버 공격, 위협의 억지, 방어는 물론 신속한 회복력의 기반임
  - 국방체계의 디지털 전환은 기기, 체계, 네트워크뿐만 아니라 운용 전반에 있어서 상호운용성을 필요로 하는 동시에 사이버 리스크를 증대시키고 있음
  - 표준화, 개방화, 연결성에 기반한 상호운용성은 디지털 기반 무기체계가 다차원, 초영역 전구공간에 대한 작전적, 전술적 효율성, 효과성의 기반임
  - 아울러, 사이버 공격, 위협으로부터의 벙어와 회복력 역시 개방적인 상호운용성에 있으며, 위협탐지, 방화벽, 바이러스 백신, 데이터 백업, 디지털 모듈과 기술, 공급망 등 개방적 상호운용성은 고도화되는 사이버 위협(특히, C-C 작전 영역)에 대응하는 핵심 전략임

- 미국은 인태전략, AUKUS Pilla II, 나토, 일본 등과 집단적 사이버 안보 목표를 공유하고 전략, 작전, 기술 등 통합적 사이버 능력 구축을 위해 협력하고 있음

〈표 5-5〉 사이버 집단안보 협력 목표

구분	사이버 동맹협력의 세부과제(예시)
미일방위협력지침 (2015)	· 사이버 공간의 안정적인 사용 보장협력 · 사이버 위협 및 취약성에 대한 정보 공유 · 자위대와 미군의 임무완수를 위한 인프라, 서비스, 훈련 협력
미영 사이버집단안보	· 디지털 공간의 자유민주적 삶의 보호를 위한 전략적 관여 · 집단적 방위와 억지를 위한 사이버 공간에서의 연합작전
쿼드 (2022)	· 쿼드 사이버안보 파트너십 · 소프트웨어 공급망과 사용자 데이터 보호를 위한 사이버 안보 · 디지털로 작동하는 제품과 서비스에 대한 공급망 안전성
AUKUK Pilla II	· 공급망 탄력성, 우주협력, 사이버, 데이터 절취, 가짜뉴스, 허위조작정보, 주요기반시설 보호, 양자컴퓨터, 양자컴퓨터 협력 · 최첨단 미사일과 방위산업기술 공유

○ 다원적, 다자적 사이버 안보협력에 기반한 사이버 집단안보체계는 1) 한국의 통합적 사이버 군사능력 강화, 2) 한미동맹 사이버 안보협력, 3) 한미일 및 다자적 사이버 안보협력이라는 세 가지 핵심 요소를 기반으로 구축

- 1차적으로 북핵위협 및 사이버·전자기 능력을 통합하여 사이버 안보위협에 대응하는 사이버 전략, 능력 및 기술적 수단 등 한국의 사이버 군사전략을 혁신
- 한미 사이버 동맹협력에 기반하여 한미일, 인태지역, 나토, 사이버 안보 국제기구 및 지역 국가와의 복합적인 안보협력 확대
- 인태전략, AUKUS Pilla II와 연계한 사이버 안보협력에 있어 일본이 추구하는 공적안보지원(OSA)를 참고할 수 있으며, 한일간 사이버 OSA의 공동 추진도 검토 필요
- 사이버 정책협의, 사이버 훈련 등 양자, 소다자, 다자체제의 사이버 군

사훈련 네트워크 주도 및 훈련 참여

○ 사이버 집단안보의 민군협력과 함께 방위산업의 연구개발, 무기수출 등 국내외의 사이버 안보 관련 이해관계자를 포괄하는 사이버 안보 혁신 네트워크(Cybersecurity Innovation Network) 차원에서 사이버 집단안보 체제 구축

- 무기체계의 개념, 설계, 생산, 수출단계에서 사이버 안보를 포함한 방위산업 기반 강화하고, 디기털 기반 무기수출과 사이버 전략, 기술을 일체화할 필요 있음
- 무기체계-사이버 안보를 일체화한 방위산업 수출전략은 사이버 집단안보확장 전략

5. 국방 사이버 전문인력 양성

○ 사이버 역량은 디지털 기반 무기체계, 지휘체계 및 부대 운용의 기초소양으로 병과 단위의 훈련에서 탈피하여 공통 핵심 직무역량으로 개편하여 통합적 교육체계 구축

- 사이버 능력의 강화를 위해서는 개방적 상호운용성에 기반하여 사이버 안보 및 디지털 안보에 대한 지식, 역량을 갖춘 인재 확보가 필수적인 과제임
- 각군 병과교육에서 사이버 작전에 대한 리터러시(cyber operation literacy) 공통교육(보안 및 DCO 기초) 및 각군 전투병과(보병(특수전), 기갑, 포

병, 정보 등)의 경우 NO작전 및 보안차원을 넘어 DCO작전 및 OCO 작전 통합교육

○ 사이버 안보 혁신 네트워크 기반 국방 사이버 전문인력 인재 양성

- 개방적 상호운용성 기반 교육을 위해서는 민-군-관뿐만 아니라 사이버, 디지털 관련 연구기관, 방위산업 등과 공동 교육, 훈련 및 교류 등의 프로그램 확대
- 사이버 안보 관련 민간기관, 방위산업과의 협력적 인재 양성, 교류체계 체계 구축
- 일본 자위대는 2021년부터 사이버 영역에서 전문역량을 갖춘 민간 부문의 인재를 '사이버 안보 총괄 어드바이저'로 채용하고 있으며, 사이버 안보 관련 예비자위관을 확보하여 운용
- 국방 사이버 PMC: 국방 전문인력의 양성을 위해 군은 인재양성 협약을 체결(고려대 국방사이버학과)했으나, 처우조건, 자기계발 등의 비교열위에 따라 민군 협력 인재양성 기반의 위기 초래
- 민간 수준의 보상과 처우조건을 유지하되 국방 사이버 안보 서비스의 핵심 기능을 수행하는 사이버 안보 PMC의 육성을 검토할 필요 있음

○ 한미동맹, 사이버 집단안보 협력국가, 국제기구와의 공동 인재양성 및 교육훈련 프로그램 확대

- 2022년 발표된 사이버 전문인력 10만 양성계획을 미국 및 주요국의 사이버사령부 및 교육기관과의 교육, 훈련, 연수 등 사이버 안보관련 공동 프로그램으로 확대
- (정치적, 사회적 인식을 고려할 때) 한미일 국방 사이버 전문인력 양성 프로

그램을 한미일 안보협력을 선도하는 프로그램으로 검토

- 아세안, 무기수출국과 사이버 안보역량에 대한 OSA 시행 등

제6장

사이버전 수행역량 강화와 공세적 방어

설 인 효 | 국방대학교 전략학부 교수

1. 사이버전 전략 및 전술 수행 체계와 기술 고도화
2. 사이버전 역량의 통합 운용과 작전 수행체계 구축
3. 공세적 사이버 방어 및 대응 개념 정립
4. 사이버전 지휘통제체계 수립
5. 사이버전 무기체계 개발 및 전력 체계와 핵심 기술 고도화

제6장

사이버전 수행역량 강화와 공세적 방어

설 인 효 | 국방대학교 전략학부 교수

배경과 구성

- 새로운 기술의 발전, 미중 전략경쟁 심화되는 상황에서 미래전 논의 및 새로운 작전개념 모색이 가속화되고 있음
- 최근 진행되고 있는 우크라이나 전쟁, 이스라엘-하마스 전쟁은 전쟁의 패러다임이 변화하고 있음을 보여주며 사이버·정보·전자전의 수행 패러다임도 변화하고 있음을 보여줌
- 미국을 비롯한 군사 강대국들은 '다영역 작전개념'에 입각하여 사이버전 수행 개념을 변화시키고 있으며 이에 입각한 무기체계, 조직, 인력상의 변화를 빠르게 추진하고 있음
- 인공지능은 인간의 활동 방식 전반을 변화시킬 것이며 전쟁 패러다임을 바꾸고 사이버전 수행 방식과 체계도 변화시켜 나갈 것임
- 이처럼 높은 불확실성 하에서 국제질서의 진영화 추세로 인해 미래 군사 위협은 더욱 다각화, 복합화될 것으로 예상되며 이에 대응하기 위해 사이버·정보·전자전 전략의 혁신적 업그레이드가 필요함

- 제6장의 구성은 아래와 같은 다섯 가지 항목을 중심으로 함

  1. 사이버전 전략 및 전술 수행 체계와 기술 고도화

  2. 사이버전 역량의 통합 운용과 작전 수행체계 구축

  3. 공세적 사이버 방어 및 대응 개념 정립

  4. 사이버전 지휘통제체계 수립

  5. 사이버전 무기체계 개발 및 전력 체계와 핵심 기술 고도화

1. 사이버전 전략 및 전술 수행 체계와 기술 고도화

○ 전쟁 패러다임 변화를 반영한 사이버전 전략 및 전술 수행체계 재편이 긴요함. 이와 같이 재편된 사이버전 전략, 전술 이행에 필요한 핵심기술의 단기적, 중장기적 확보를 위해 기술 고도화 전략의 구축 및 체계적 이행 필요

- 미중 군사혁신 경쟁이 치열하게 진행되고 있는 현실을 고려할 때 전쟁 패러다임 변화에 따른 사이버·정보·전자전 전략의 근본적 재검토가 필요함
- 미중 전략경쟁 구도 하에서 '평시 – 회색지대 분쟁 – 전시'의 경계가 모호해지고 있으며 비물리적 공격과 물리적 공격의 상호 연계, 민간 영역 자산의 원활하고 효과적인 활용, 사이버 의용군 등 자발적 참여 활용 등이 새로운 과제로 부각되고 있음. 국제적 진영화 진행에 따른 국제 연대 및 협력적 대응도 새로운 전략적 과제임

○ 최근 진행되고 있는 전쟁의 경험으로부터도 많은 교훈이 도출되고 있음

- 우크라이나 전에서 사이버전과 관련된 교훈은 다음과 같음
  · 긴밀한 국제 사이버 지원 체계의 구축
  · 다층적 사이버 방어 체계의 중요성
  · 정보전에서의 주도권 확보
  · 사이버 의용군과의 협력 활용
  · 비대칭적 사이버 공격 대비
  · 드론 및 자동화 기술의 사이버 통합
  · 사이버 복원력 강화
  · 민간 인프라 보호 및 복구 협력 체계 구축
  · 사회적 회복탄력성 증대
  · 위기 대응 프로토콜의 정비
- 이스라엘-하마스 전에서 사이버전과 관련된 교훈은 다음과 같음
  · 초기 탐지와 대응 시스템 강화
  · 공공 및 민간 인프라 보호 강화
  · 사이버 심리전과 정보전 대응 전략 수립
  · 드론 및 자동화 기술의 통합
  · 사이버 방어 체계의 발전과 교육 강화
  · 국제 사이버 협력과 연대 강화
  · 사이버 위협 예측 및 분석 능력 강화

○ 현대전은 평시-위기발생-회색지대-전쟁의 구분이 불명확해지고 있으며, 따라서 각 시기에 적용되는 국가 사이버 역량 역시 끊김이 없이(seamless) 작동할 수 있어야 함. 각 시기의 주도 역량은 유연하게 대응하고 사태 전

개 가능성을 다른 주체들과 공유해야 함

- 적은 더욱 기습적 방식으로, 기존과 다른 창의적 방식으로 전쟁을 개시할 수 있으므로 위기 도래 시 주요 관련 기관에 대한 신속한 전파가 가능하도록 해야 하며 사태를 면밀히 모니터 하면서 준비 태세를 강화하도록 해야 함
- [전략적 수준]의 대규모 사이버전의 경우 1) (피해의 범위와 규모를 통제할 수 없다는 점에서) 주변국 피해 등 의도하지 않은 피해가 발생할 수 있다는 점, 2) (제한전을 수행하고자 할 경우) 사회 기간 시설 대규모 마비 등 위기가 지나치게 고조될 수 있다는 점, 3) 아직 파악되지 않은 상대의 전략적 수준의 대규모 공격을 유발할 수 있다는 점 등에서 실제 사용은 제한적임

  ※ 최근 전쟁 및 분쟁 연구에서 나타나는 현상이나 한반도 상황에서는 다른 양상을 보일 가능성도 존재함

- 그러나 전략적 수준의 사이버 역량 확보는 여전히 중요함. 1) 북한의 경우 비대칭적 비물리전 수단인 사이버 공격을 대규모로 감행할 가능성이 크며, 2) 상대가 전략적 수준의 사이버 공격 수단 사용을 주저하도록 하기 위해서는 실제로 높은 수준의 전략적 사이버 역량을 갖추고 있어야 하기 때문임
- 따라서 [작전적, 전술적 수준]에서 적의 정보 흐름을 차단하고 아측의 정보를 보호하는 작전을 효과적으로 수행하는 것이 핵심임. 현대전은 정보의 유통을 기반으로 수행되기 때문에 지, 해, 공 등 모든 영역에서 수행되는 작전은 정보의 유통이 보장되어야 하며 적의 정보 유통 방해·차단을 통해 압도적 우위를 확보할 수 있음

○ 사이버 공격에 대응하는 데 있어서 민간 영역과의 협력은 사활적으로 중요한 일이 되었음. 따라서 위기 발생이 감지된 경우 국가 기간시설과 관련된 민간 기업들에 대해 조기 경보를 발령할 뿐만 아니라 일정한 조건하에서 사이버 대응에 기여할 수 있는 민간 주체들을 사전에 식별하고 이들과 신속하고 효율적인 협력 방안을 모색하여 정기적 훈련을 실시해야 함

※ 충무사태 시 동원 관련 조항 개정 또는 보완 필요

- 최근 전쟁에서 관측되는 바와 같이 명시적 국제공조뿐만 아니라 사이버 의용군의 자발적 협력을 독려하고 이끌어 낼 수 있는 역량을 갖추어야 하며 이를 위한 매뉴얼을 작성하고 유사시를 대비한 훈련을 실시해야 함
- 이와 같은 사이버전의 전략적, 전술적 수준의 운영 발전을 위해서는 관련 기술의 지속적인 발전이 반드시 필요함. 단순히 일부 사이버 무기체계의 개발뿐만 아니라 사이버전 운영 전반을 현대화하고 혁신할 수 있는 기술 및 기반체계 구축에 대한 지속적 투자, 국제협력 강화가 반드시 필요함

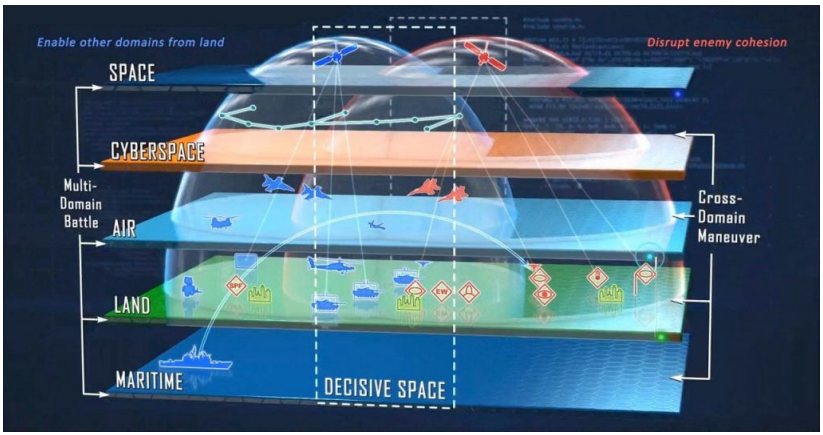
※ 단순한 사이버 무기체계 기술뿐만 아니라 전반적 운영체계 기술 발전에 투자해야 함

2. 사이버전 역량의 통합 운용과 작전 수행체계 구축

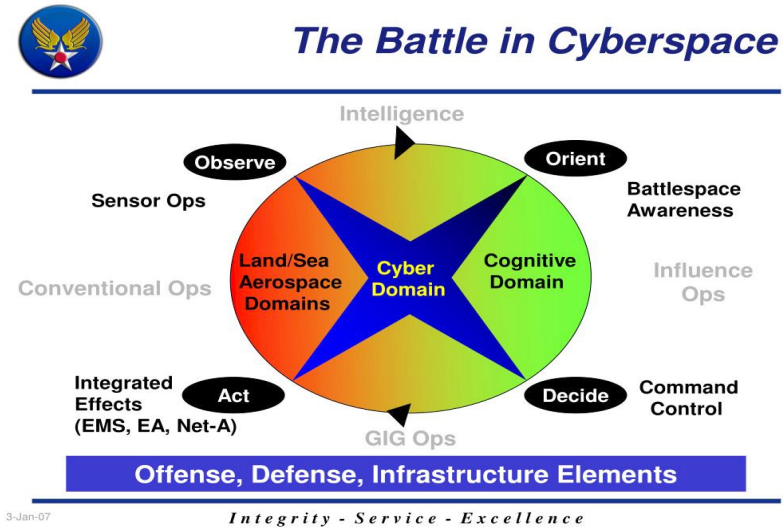
○ 다영역작전 개념에 입각한 사이버전 수행을 위해서는 새로운 역량과 작전 수행 개념이 필요함. 6개 전장 영역에 존재하는 모든 역량의 통합적 운영 관점에서 사이버 작전 수행체계를 재구축해야 함

- 현대 전장은 다영역 공간이며 지상, 해상, 공중, 사이버, 우주, 전자기장 영역에 존재하는 모든 전력을 동시, 통합적으로 활용하는 것이 승리의 요체가 될 것임

〈그림 6-1〉

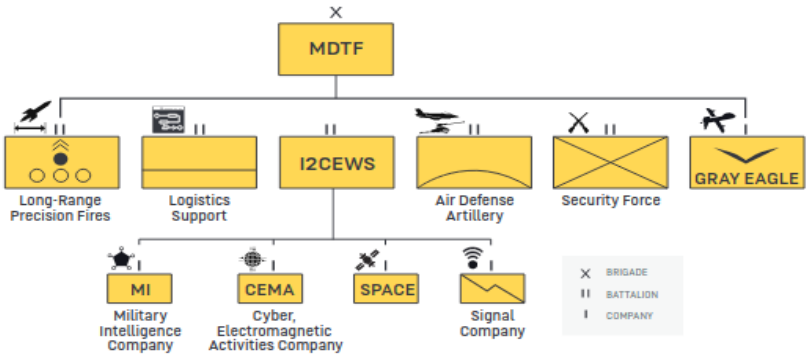


〈그림 6-2〉



- 장거리 정밀타격 보편화로 거리의 경쟁이 시간의 경쟁으로 전환되고 있는 현대전에서 아측의 피해를 최소화하고 최소 규모의 물리적, 비물리적 타격으로 최대 효과를 거두는 '효과 중심 작전'이 추구되고 있으며, 이를 위해 '사이버·정보·전자전'을 앞세운 '다영역 동시 통합 작전 수행 개념'이 새로운 표준으로 부상하고 있음
- 6개 전장을 가로지르는 '교차 영역 기동(cross domain maeuver)'는 현대적 다영역 작전의 근간인바 <그림6-1>이 보여주는 바와 같이 영역 간 교차는 모두 사이버 공간을 통해서 가능해짐
- 따라서 탐재-추적-결심-타격으로 이어지는 전투 수행 전 과정에서 사이버 영역은 연결과 통합의 기능을 수행하며 단순히 수동적/수세적 사이버 대응을 넘어 현대전의 성공적 수행을 보장하는 핵심 영역으로 자리매김해야 함

〈그림 6-3〉



- 다영역 작전 수행을 위해 편성된 '다영역 임무 부대(multi domain task force, MDTF)'의 구성은 사이버, 전자전, 우주전, 정보전이 전략 및 작전 수준뿐만 아니라 작전 및 전술 수준에서도 통합적 방식으로 운영될 것임을 잘 보여주고 있음
- 사이버 방어, 공격 작전은 특정한 조건 하에서 단독으로 시행될 수 있으나 우주, 전자기장 작전과 동시에 시행되어 상호 상승효과를 강화해야 하며 지상, 해상, 공중 작전과의 긴밀한 연계 속에서 시행되어야 함
- 즉 기존의 지상, 해상, 공중 작전 시행 전후 사이버, 우주, 전자기장 공격이 동시 병행적으로, 동기화된 방식으로 구사됨으로써 적의 대응 역량을 약화하고 아측의 공격효과를 최대화할 수 있어야 함. 작전시행 전 기간(full spectrum)에 걸쳐 아측 전력을 사이버 공격으로부터 효과적으로 방어할 수 있어야 함
- 이와 같은 작전 시행을 위해서는 우주, 전자기장 영역의 작전뿐만 아니라 지상, 해상, 공중 작전의 특성과 교리에 대해 이해해야 하며 사이버전의 특성과 시행 방식에 대해 다른 공간의 전력들과 지휘관이 충분히

이해할 수 있도록 사전에 교육과 훈련을 충분히 실시해야 함

- 특히 유사시 이와 같은 다영역 작전 시행을 위해 지휘관에게 필요한 조언을 할 수 있는 전문가 집단을 양성할 수 있어야 함

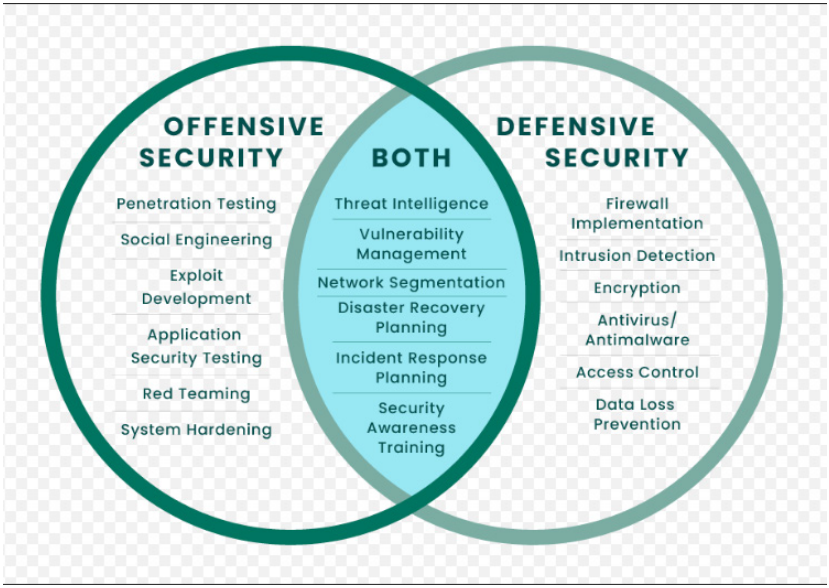
※ 전투 수행 중 군 지휘관에 대한 사이버와 전자전 영역의 전문적 조언을 위해 미 육군은 '사이버 전자기영역 활동팀(CEMA: Cyber and Electro-Magnetic Action)'을 발전시키고 있는바 '한국형 CEMA(K-CEMA)'의 육성과 활용이 필요함

3. 공세적 사이버 방어 및 대응 개념 정립

○ 사이버 공격 발생 시 대응하는 개념에서 발생 자체를 차단하고 신속한 대응을 가능하게 하는 공세적 사이버 방어 개념 정립 및 수행 체계 구축 필요함. 또한 사이버전 수행, 대응 체계를 전쟁 패러다임 변화에 맞춰 재편해야 함

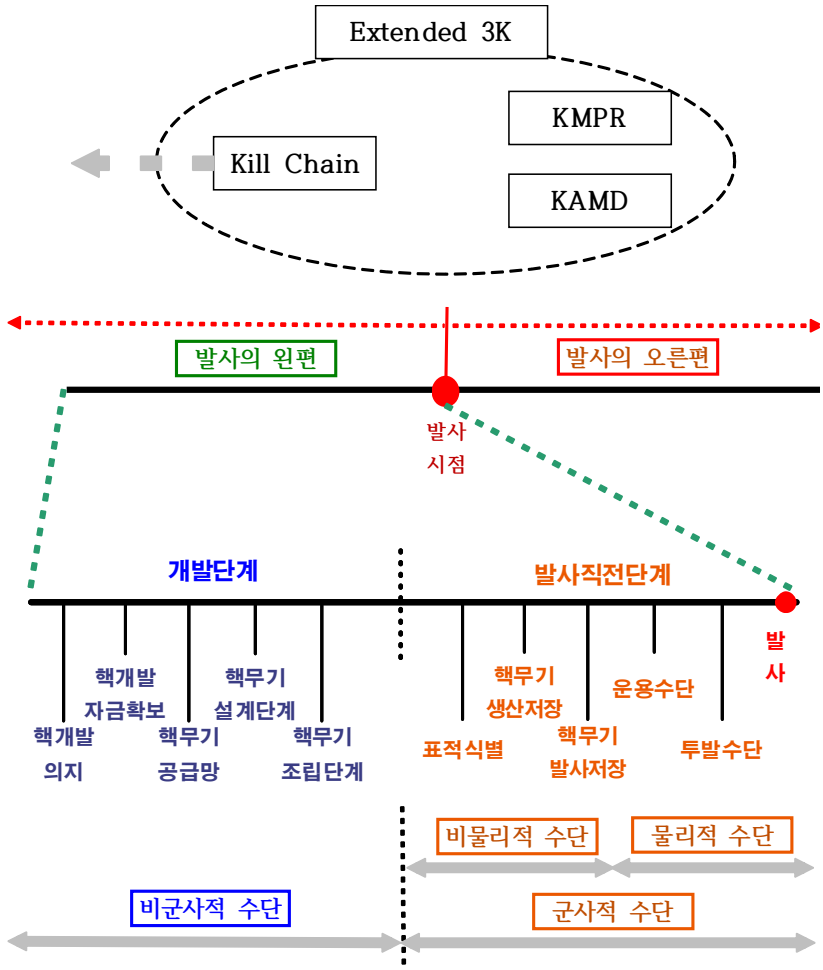
- 향후 사이버 공격은 더욱 은밀한 방식으로 다양한 규모로 감행될 것이며 이에 대해 충분한 방어와 대응이 이루어지지 못할 경우 국가안보 역량의 심각한 저하가 불가피할 것임
- 따라서 사이버 공격의 조기 감지 및 신속한 대응은 국가안보의 기반이 될 것인바 조기 경보 체계의 지속적인 발전과 확대가 긴요함

〈그림 6-4〉



- 사이버 공격이 감지, 식별되는 경우 필요에 따라(기준 설정 필요) 관련 체계 및 역량 운영 기관에 정보를 공유하고 다양한 수준과 단계에 따른 대응으로 적이 공격을 확대하지 못하도록 해야 함
- 비물리적 공격에 대해서는 현행 법체계 및 여건상 비물리적 공격으로 대응하는 것이 유리하다는 점에서 사이버 공격의 수단과 방식을 지속적으로 다양화해 나가야 함

〈그림 6-5〉



- 상술한 바 변화된 전쟁 패러다임에 입각하여 잠재 적의 사이버 공격이 일정한 수준을 넘어설 경우 조기 경보, 선제적 대응에서 더 나아가 민간 영역에 대한 경보, 민간 영역과 공동 대응, 국제적 공동 대응, 국제 여론에의 호소와 자발적 사이버 의용군 활동 장려 등을 단계적으로 이

어나갈 수 있을 것임

- 나아가 적의 공격이 임박한 경우 적의 공격력을 먼저 공격하여 피해를 최소화하고 적이 공격을 주저하도록 할 피해를 유발하는 적극적이고 공세적인 작전을 구상함
- 이와 같은 역량의 보유와 정기적 연습을 통한 시연은 그 자체로 방어 및 억제 효과를 발휘할 수 있는바 이러한 억제력을 효과적으로 활용하는 방안을 마련해야 함
- 마지막으로 적의 핵 공격 임박 시 핵 무기체계 발사 전 타격이 필요한 바 이는 전쟁 책임과 관련하여 비물리적 공격을 우선 시행해야 하며 이를 위해 효과적인 사이버 공격 전략 발전이 필요함
- 보다 광범위한 발사 전 단계에 대한 비물리적 공격 방안은 향후 북핵 억제의 핵심이 될 확장된 3K 작전의 중요한 전력이 될 것임

4. 사이버전 지휘통제체계 수립

○ 다영역 작전 수행을 위해서는 사이버전 지휘통제체계 수립이 핵심적 근간이며 이를 위해 '사이버 전장 가시화', '합동 전장 가시화 체계' 구축 및 통합이 필요함. 전쟁 패러다임 변화에 부응할 수 있는 첨단 사이버 지휘통제체계 수립을 기획하고 체계적, 단계적으로 추진해 나가야 함

- 사이버 지휘통제체계 수립은 현대 및 미래전의 기본 패러다임인 다영역 작전 수행의 근간이 되므로 미래 지향적인 지휘통제체계 수립을 단기적으로 뿐만 아니라 중장기적 관점에서 체계적으로 구축해 나가야 함

- 한국 군의 현 수행체계는 다음과 같이 평가할 수 있음
  · 한국 군은 합참이 사이버작전사령부를 지휘, 감독하여 사이버작전에 관한 관제, 상황처리, 대응작전을 수행하며 작전 수행을 위한 지침과 교리, 사이버 작전계획 등을 총체적으로 발전, 통제
  · 사이버작전사령부는 전군 차원의 상황인식, 종합관제 및 상황관리 임무를 수행하면서 수집, 분석한 사이버 위협정보를 전군에 제공하고, 침해사고 예방, 탐지, 대응, 복구 등의 방지 활동도 시행
  · 각 군의 경우 제대별로 보유한 사이버 능력을 고려하여 CERT 혹은 사이버 방호센터를 통해 네트워크 작전 위주로 작전을 수행하며 필요 시 합참에 공세적 사이버 작전에 필요한 첩보 및 정보, 데이터를 제공함
  · 한국은 2000년도 이후 본격적으로 사이버·전자전을 대비하여 핵심 조직인 사이버작전사령부는 창설 당시, 3-400명 규모에서 현재는 1,000여명 규모로 2배 이상 확대되었고, 기만/잡음/복합/다중 재밍 기법을 적용한 ALQ-W200K 등을 개발하여 국군의 주력 전투기인 KF-16D 전투기에 탑재해서 운용 중임
  · 우리 군은 여전히 사이버·정보·전자전이 합동작전의 예외적 일부, 별도의 분리된 부분으로, 전체 작전 체계와의 연계 속에서 이루어지고 있지 못함
  · 이와 같은 다영역 작전 수행을 위한 여건과 기제, 조직도 충분히 갖춰져 있지 못한 상황임

○ 국제질서의 전반적 진영화와 북중러 협력의 가시화를 고려할 때 중장기적으로 북한 역시 네트워크 기반 전쟁을 수행하게 될 가능성이 크며 중국과 러시아의 묵시적, 명시적 지원 하에 전쟁을 수행할 가능성도 배제

할 수 없음.

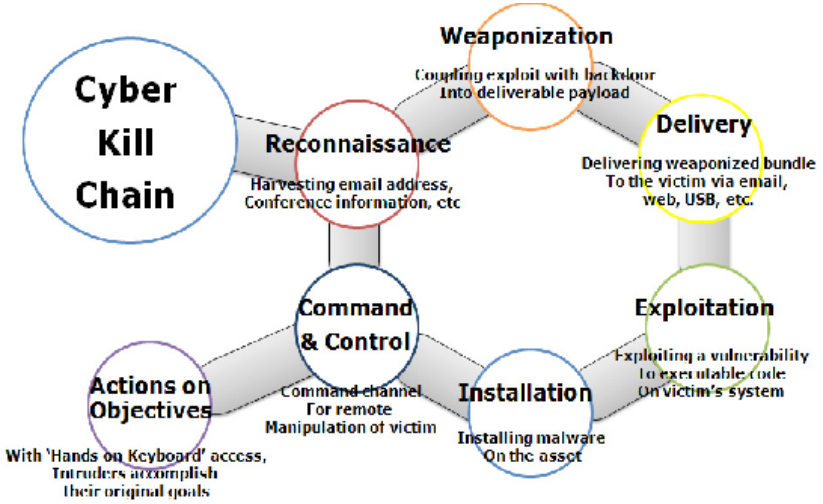
- 진영 간 대결이 격화될 경우 중국, 러시아와의 직간접적 충돌 가능성도 상정하지 않을 수 없을 것임
- 따라서 세계적 군사표준으로 부상하고 있는 미래적 작전수행 개념에 적합한 사이버·정보·전자전 수행체계와 작전개념, 전문 인력 양상 추진에 주력해야 함
- 군사영역에서는 북한을 상대로 수세적 방어 위주의 작전개념에 머물지 말고 공세적 작전개념과 역량을 발전시켜 주변 강대국에 대한 수적 열세를 만회하는 수단으로 활용해야 함
- '사이버 전장 가시화 체계'를 지속적으로 확대하고 강화시켜 나가야 하며 인공지능 등 신기술 적용을 통해 신속성과 범위의 확대, 정확성 증대 등을 계속 지향해 나가야 함
- '사이버 전장 가시화 체계'는 '합동 전장 가시화 체계'에 통합될 수 있어야 하는바 이를 전제로 한 체계 구축 및 개선, 조정이 필요함
- 궁극적으로 합동 지휘관이 전장 전반에 걸쳐 사이버 위협의 존재 및 양상을 인식할 수 있도록 하고 이에 대응할 수 있는 사이버, 우주, 전자전 대응체계와 지, 해, 공 상의 물리적 대응체계 전체를 식별할 수 있도록 발전되어 나가야 함
- '사이버 전장 가시화 체계' 및 '합동 전장 가시화 체계'는 '효과 기반 작전' 및 '결심 우위' 보장의 핵심 기반이 될 것인바 데이터 아키택쳐 관점에서 미래 지향적으로 설계되어야 하며 대규모 정보의 실시간 동시처리가 가능한 수준으로 구축되어 향후 전장 활용이 가능한 알고리즘 발전과 전쟁 수행 시 결정 우위를 보장할 수 있는 정보 유통을 가능하게 해야 함

5. 사이버전 무기체계 개발 및 전력 체계와 핵심 기술 고도화

○ 미래 첨단기술을 반영한 사이버전 신무기체계 개발 노력을 지속해야 하며 전력 체계 발전도 추진해 나가야 함. 이와 관련된 핵심기술 고도화를 위해 국방 사이버 무기체계 개발 생태계를 구축하고 관련 국제적 협력도 고도화해 나가야 함

- 사이버 방어 및 공격의 성공적 수행은 국가 안보 수호의 핵심 기반이 될 것이며 이의 성공적 수행을 위해서는 무기체계 개발 및 전력 체계 강화가 반드시 선행되어야 함
- 이와 관련된 기술은 특성상 외부 노출이 불가하여 국제적 협력에도 제한 사항이 발생할 가능성이 높은 바, 핵심 기술 고도화를 위한 국가 차원의 지원과 정책의 수립이 반드시 필요함
- 한국 군은 군사전략적 관점에서 미래 사이버 기술 및 무기체계가 지향해 나가야 할 방향을 설정하고 이러한 방향의 무기체계 개발 및 기술 발전이 가능하도록 국방 연구개발 투자를 효과적으로 활용해야 함
- 관련 핵심 기술의 고도화를 위해서는 국내 기술 및 무기개발 생태계의 구축이 반드시 필요한 바, 민간 영역에서 자생할 수 있을 뿐 아니라 군사적 잠재성이 높은 기술을 식별하고 이에 대한 집중적이고 중장기적 투자를 통해 국내 생태계가 안정적으로 구축되도록 지원해야 함
- 기초 및 기반 단계의 국제협력은 국내 기술 기반 확대 및 강화에 긴요한 바 주요 동맹 및 우방국가와의 기술 협력 및 교류를 장려하고 이를 뒷받침할 수 있는 제도적, 정책적, 예산적 지원을 강화해야 함

〈그림 6-6〉


Cyber
Kill
Chain
Reconnaissance
Harvesting email address,
Conference information, etc
Weaponization
Coupling exploit with backdoor
Into deliverable payload
Delivery
Delivering weaponized bundle
To the victim via email,
web, USB, etc.
Exploitation
Exploiting a vulnerability
To executable code
On victim's system
Installation
Installing malware
On the asset
Command
& Control
Command channel
For remote
Manipulation of victim
Actions on
Objectives
With 'Hands on Keyboard' access,
Intruders accomplish
their original goals

제7장

사이버 불법 활동·영향력 차단 및 사이버 기반 조성

윤 정 현 | 국가안보전략연구원 연구위원

1. 사이버 안보 컨트롤타워의 효과적 가동
2. 사이버 안보의 범부처 공조 체계 정비
3. 사이버 안보 분야 민관협력 체계 정비
4. 사이버 안보 외교의 추진체계 정비
5. 사이버 안보 분야 법제도 정비

제7장

사이버 불법 활동·영향력 차단 및 사이버 기반 조성

윤 정 현 | 국가안보전략연구원 연구위원

배경과 구성

- 최근 사이버 공간에서는 북한이 벌이고 있는 다차원적 불법활동의 피해 규모가 급증하고 있으며 이들의 직간접적 영향에 대한 면밀한 진단과 체계적 대응이 시급해지고 있음
  · 특히, 북한의 사이버 불법 활동들은 안보를 직접적으로 위협하는 핵 능력의 강화로 이어지며, 이는 북한 체제 공고화라는 악순환으로 귀결됨
  · 보다 정교한 형태로 진화하고 있는 북한의 사이버 영향공작은 사회 혼란을 유발하고 나아가 민주주의를 위협하는 은밀한 위협으로 자리잡고 있으며, 사이버 공격역량과 결합 시 보다 심각한 안보적 문제가 될 수 있음
- 북한의 다차원적 사이버 불법활동·영향력 증가는 우리로 하여금 방어역량 강화를 넘어 억지력 확보를 위한 능동적 대응책을 모색할 필요성을 제기함
  · 특히, 현 정부는 향후 국가안보·국익을 위협하는 악의적 사이버 위해

활동에 대해 공세적 대응으로 패러다임을 전환함으로써, 국가 사이버안보 수준을 격상시킬 것을 천명한 바 있음

- 북한과 주요 도전세력의 사이버 불법활동이 초래하는 정치·경제·사회적 위협과 침투 메커니즘에 대한 면밀한 분석이 필요하며, 내부의 사이버 역량 강화뿐만 아니라 글로벌 사이버 공조체계 마련이 시급함
  · 초국적 사이버 위협에 대한 정보 수집·분석 기반을 강화하고, 글로벌 사이버 공조체계 구축을 위한 세부 실천 방안을 모색해야 함
- 공세적 관점에서 우리의 대북 사이버 역량을 강화하기 위해서는 북한 내부의 디지털 환경 실태에 대한 면밀한 분석과 활용 방안에 대한 연구가 병행되어야 함

- 제7장의 구성은 아래와 같이 다섯 가지 항목을 중심으로 함
  1. 가상화폐 탈취 및 경제적 불법행위 차단
  2. 북한의 사이버 영향공작 대응체계 마련
  3. 대북 사이버 제재 공조체계 구축
  4. 북한 사회의 디지털 억압 실태 개선
  5. 북한 사회의 디지털 환경 실태 진단 및 활용방안 탐색

1. 가상화폐 탈취 및 경제적 불법행위 차단

○ 암호화폐 시장의 성장과 함께 북한의 암호화폐 탈취 시도 역시 지속적으로 증가하여 현재 가장 많은 암호화폐 공격을 시도하는 국가로 알려져

있음

- 2016년 이후 부과된 강력한 미국·UN 대북제재에 대한 회피방안으로 암호화폐 공격에 관심을 두기 시작하여 은행과 암호화폐거래소 등 금융기관 쪽으로 사이버 공격의 방향 전환
- 북한은 러시아, 중국과 함께 국가배후의 사이버 공격을 감행한다는 점에서 공통점을 갖지만 재정적 목적의 사이버 공격에 주력한다는 점에서 차별성을 지님

○ 북한이 사이버 공격을 통해 탈취한 암호화폐의 상당 규모(절반 가량)가 핵미사일 개발자금으로 활용된다고 의심받는 상황으로, 암호화폐 공격은 금전적 피해와 안보위협으로 동시 작용

- 특히 향후 북러협력을 통해 핵미사일 프로그램의 기술적 발전과 함께 암호화폐 공격을 통한 외화수입 확충이 동시에 이루어질 경우 심각한 안보위협이 될 수 있기 때문에 대비책 마련 절실

○ 최근 북한의 가상화폐 탈취 현황 및 특징을 살펴보면, 원 늘어나는 해킹 시도와 줄어드는 외화수입을 들 수 있음

- 2022년 암호화폐 해킹금액은 최고액을 기록했으나 2023년은 대폭 감소
  · 블록체인 분석업체 체이널리시스(Chainalysis)는 2023년 북한연계 해킹조직이 암호화폐 플랫폼 20곳을 해킹해 10억 달러를 빼냈다고 추산했으나 이는 2022년 17억 달러에 비해 40% 이상 줄어든 수치
  · 반면, 북한에 해킹당한 플랫폼은 2022년 15곳에서 2023년 20곳으로 증가하여 해킹 시도가 늘어난 데 비해 확보한 금액은 줄어든 것으로 추정

· 암호화폐 믹싱 과정에서 어려움을 겪고 있다는 증거이거나, 암호화폐 업체들이 보안을 강화하고 있다는 의미로 해석 가능[1)]

○ 금전적 목적의 랜섬웨어 공격 증가

- 2022년부터 재정적 목적의 전방위적 랜섬웨어 공격 기승

· 워너크라이(WannaCry 2.0)의 주요 목표가 사회적 혼란 조성, 적성국에 대한 경제적 타격이었다면 최근 랜섬웨어 공격은 자국의 통치자금 마련에 초점

· 외화수입 확보가 목표이기 때문에 개인보다는 지불 능력이 있는 병원, 대기업 등이 주요 표적이지만 필요한 경우 개인과 영세기업까지 공격 확대

· 마우이(Maui)와 홀리고스트(HOlyGhOst) 등 새로운 랜섬웨어를 직접 개발하여 전 세계를 상대로 피해를 일으켰으며 안다리엘(Andariel)이 배후로 있을 것으로 추정

○ 러시아와의 사이버 협력 증대 가능성

- 2023년 9월, 러북정상회담 이후 양국간 협력이 전방위적으로 이루어지면서 북한이 훔친 암호화폐를 세탁하기 위해 러시아를 활용하는 정황이 포착됨

· 추적을 피해 암호화폐를 소량씩 장기간에 걸쳐서 세탁을 해야 했던

1) 미국 정부는 믹서 업체 '토네이도 캐시,' '신바드'를 제재하고 암호화폐 현금화를 도운 장외거래 업자들을 제재 대상에 올려놓음으로써 북한의 현금화를 막았기 때문이라고 분석.

북한은 그동안 거래처를 찾기 어려워 세탁 대가로 훔친 금액의 1/3만 수령

· 러시아의 암호화폐 거래소를 통해 우호 가격에 대량의 암호화폐를 안정적으로 세탁할 수 있을 것이며 러시아 또한 브로커 비용을 챙겨 외화수입 확보 가능

· 가상세계에서 국가간 협력 정황은 포착과 증명이 어려워 랜섬웨어 기술 이전, IT 인력 송출 등 러북간 사이버 분야 협력이 대북제재 위반 루트로서 적극 활용될 가능성

※ 북한 IT 인력이 러시아의 첩보전을 보조함으로써 외화를 습득하거나 첩보 능력을 획득하여 한국에 활용할 가능성도 배제 불가

○ 이에 대한 대응 방향을 살펴보면, 먼저 암호화폐 탈취 과정에서의 적의 취약점 역공격할 수 있는 카운터해킹 역량 증진 및 이를 위한 전문적인 화이트해커 양성 또한 체계적으로 이루어질 필요가 있음

- 미국의 FBI와 법무부의 협력사례를 참고하여 국가정보원이 주도하고 법무부의 협력하에 랜섬웨어 범죄자 및 불법 환전자에 대한 검거 활동 강화 모색 등

· 기술 혁신 및 지능형 플랫폼 관리를 통한 북한 정권의 신속 대처 능력 무력화를 통해서 대체 플랫폼 선제 차단, 사전적 규제 조치, 혁신적 추적기술 개발 등

※ 북한 정권이 암호 화폐를 주요 수단으로 활용하는 것도 블록체인 기술의 변동성에 기인

- 디지털 금융 범죄 플랫폼 폐쇄 후 보안 체계 및 익명성이 강화된 신규 플랫폼 등장으로 자금 추적에 난황을 겪은 사례 다수인데, 2022년 독

일 하이드라(Hydra) 폐쇄 이후 다크넷 시장 변화 사례(TRM Labs 보고서), 토네이도캐쉬(Tornado Cash) 제재 후 프라이버시 코인 시장 동향,[2] 알파베이(AlphaBay) 폐쇄 후 모네로(Monero) 등장 등

○ 사이버 범죄 다각화의 민첩·유연·신속 대응 및 유관기관 간 원활·견고한 협력을 위하여, 재경부 산하 상설 「가상 자산 위험 위원회」 출범 검토

- 「가상 자산 위험 위원회」: 2022년 미 법무부가 구상한 신기술 관련 상설 위원회인 신흥기술위원회(Emerging Technology Board)와 유사한 형태로, 미 재무부가 「디지털 자산의 불법 자금 조달 위험을 해결하기 위한 실행 계획」(2022)에서 제안한 바 있음[3]

○ 민관 협력 네트워크 구축

- 공공-민간 간 사이버 보안 관련 정보의 실시간 공유를 통해 랜섬웨어 공격 패턴이나 해킹 시도를 신속하게 파악·대응
- 최근 사이버 공격 급증으로 미국 정부는 마이크로소프트사·구글사 등 민간과의 협력을 통한 시스템 보안 강화, 구체적 협력 모색[4]

2) 칩믹서(ChipMixer) 폐쇄 후 와사비(Wasabi)·사무라이(Samourai) 등 프라이버시 지갑 및 익명성 강화된 코인조인스(CoinJoins) 프로토콜 사용. 세부 내용 다음 참조: Dr. Arda Akartuna, “The Next Tornado Cash? Six Protocols Vying to Replace the Famous Crypto Mixing Service,” Elliptic, 2022년 5월 9일,

3) Margaret Haggerty, Andy Lorentz, “Addressing Digital Assets' Illicit Financing Risks: 'Supporting Actions' Still Needed to Execute Treasury's Action Plan,” 2022년 9월 30일,

4) The White House. “FACT SHEET: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity.” 2024년 6월 10일

ex) 마이크로소프트: 보안 제품 할인·지원, 무료 교육 등을 통하여 악성 사이버 공격 대비 능력 강화

ex) 구글: 보안 자문 제공 및 보안 제품 할인, 의료기관 등 수혜기관 별 맞춤 보안 솔루션 개발·제공 등

○ 사이버 대응 인프라 법제 개편 및 규제 강화

- KYC(고객 신원 확인) 및 AML(자금세탁 방지) 규제 관련 주요 법률인 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」은 글로벌 기준에는 부합하나,
- 북한의 사이버 범죄 기술·유형 전개에 따른 보완, 특히, 가상자산 법적 정의 명시, 관련 서비스 제공자로 AML/KYC 관련 규제 의무 부과 대상 확대 추진이 필요

○ 정부 차원 블록체인 분석 기술 도입으로 불법 거래 흐름 추적 및 자금 세탁 방지

- 암호 화폐는 거래의 즉시성으로 인하여 자금의 복구·회수가 제한되므로, 탈취 암호 화폐 복구 및 보호 기술 개발 필요
- 의심 거래 즉시 탐지를 위한 실시간 거래 모니터링 알고리즘 등 불법 거래 익명성 최소화 및 체계적 추적을 위한 기술 개발
- 북한이 암호화폐 탈취 과정에서 현재 북한이 가장 어려움을 겪는 '환전 프로세스'에 초점을 두어 암호화폐의 세탁·믹싱 시도를 무력화할 필요

2. 북한의 사이버 영향공작 대응체계 마련

○ 2023년 말, 김정은이 제8기 제9차 전원회의 결론에서 남북관계를 '적대적이고 교전 중인 두 국가'로 규정한 이후, 북한의 대외 전략 노선은 더욱 공격적으로 변화하고 있음

○ 북한은 그동안 주로 금전적 이익이나 민감정보 탈취, 정치적 영향력 확대를 목표로한 사이버 공격을 감행해왔으나 이제 은밀하게 사회 여론을 조성 또는 왜곡하는 '영향공작'(influence operation) 차원의 사이버 활동에 초점을 맞추고 있음

※ '영향공작(influence operation)'은 "다양한 정보 유통과 메시지 전달을 통해 타국의 여론과 정책이 자국에 우호적으로 변하도록 하는 고도의 정보전이자 심리전"

○ 북한의 영향공작은 주로 경제적, 정치적 목적을 달성하기 위해 이루어지며, 국제적 제재와 고립 속에서 자신들의 이익을 극대화하려는 전략적 시도로 해석

- 대부분은 온라인 미디어, 커뮤니티, SNS 등 사이버 공간을 통해 전개되며, 불특정 다수에 대한 은밀하고 전방위적인 공격의 행태를 보이고 있으며, 뉴미디어와 SNS를 통한 '허위정보(disinformation)'를 통해 사회 갈등을 유발 중

○ 현 시점에서 북한의 사이버 영향공작이 우리에게 위협적인 이유는 이를

감행할 수 있는 인적·기술적 역량을 보유하고 있을 뿐만 아니라 다양한 공격 노하우와 정보 자산을 연계하여 더욱 정교하고 효과적인 공작을 전개할 가능성이 높기 때문

- 향후 북한이 사이버 공간 내 사회공학적 기법을 접목한 영향공작의 강화 가능성과 국가안보 차원의 경각심 제고와 함께 기술적·제도적 대응 수단의 확보가 시급함을 시사

○ 최근 사이버 영향공작 진화 양상 및 위험성을 살펴보면, 우선 북한의 영향공작은 주로 경제적, 정치적 목적을 달성하기 위해 이루어지며, 국제적 제재와 고립 속에서 자신들의 이익을 극대화하려는 전략적 시도로 해석됨을 주목할 필요

※ 현재 북한은 사이버 공작 요원 약 1,700명과 지원·기술인력 약 4,300명을 보유하고 있는 것으로 알려졌으며, 특히 해외에서 기업으로 위장한 주요 거점을 통해 활발한 공작을 진행하는 한편, 여론 왜곡과 사회 분열을 유도하기 위해 약 300여명 이상의 댓글 전문요원이 허위정보, 역정보, 가짜뉴스 생성·유포 중인 것으로 추정[5)]

○ 2024년 5월 11일 밝혀진 북한 추정 해킹 조직 '라자루스'의 대법원 전산망과 보건복지부 공식 X 계정 해킹 사건은 표면적으로 개인정보 유출이라는 단순한 '사이버 침해사고'의 형태를 띠고 있으나 향후 사이버 영향공작 고도화에 활용될 정보수집 활동으로서의 의미도 내포

5) https://news.mt.co.kr/newsPrint.html?no=2024040416321886792&type=1&gubn=

- 북한 해킹 조직이 2021년 1월 이전부터 지난해 2월까지 법원 전산망에 침입해 유출한 대량의 데이터에는 주민등록초본, 개인회생신청서, 지방세과세증명서 등 광범위한 개인정보가 포함

○ 표면적으로 경제적 피해나 국가안보 차원의 민감정보 유출과는 거리가 먼 '보안사고'의 형태를 띠고 있지만, 사이버 영향력 공작에 악용할 수 있는 대규모 정보 자산과 소통 채널에 침투할 수 있음을 시사하기 때문

- 탈취 개인정보를 토대로 표적 집단화하여 보다 민감한 경제·사회·보건 이슈에서 허위정보 확산을 통해 국민적 혼란을 촉발할 수 있는 중대한 위험성 내포
- 이를 악용할 경우, 개인 SNS나 이메일을 더욱 손쉽게 해킹할 수 있으며, 유명인을 타겟으로한 '스피어피싱' 공격 역시 더욱 손쉽게 수행 가능

※ '스피어피싱(spear-phishing): 공격자가 사전에 특정 표적을 설정, 관련 정보를 수집·분석하여 정교한 피싱 공격을 수행하는 공격 형태

- 주요 인사들의 경우, 공격을 위해 지인, 인맥관계, 활동 정보들을 사전에 입수하고, 주변인물 등 공격 범위를 조금씩 좁혀나가는 방식을 통해 이루어지고 있음을 고려할 때, 이 같은 공공전상망 해킹 사태가 시사하는 잠재적 위험성은 더욱 심각

○ 북한의 영향공작의 또 다른 위협적인 측면은 같은 언어와 문화적 정서적 민감성을 가진 인간이 직접 개입하는 댓글 등을 통해 정교하게 이루어지기 때문

- 기계화된 가짜계정이나 '봇(bot)' 등을 이용한 러시아, 중국 등의 정보조작 규모에는 미치지는 못하나, 언어와 뉘앙스의 오류, 철자와 문법의

일관된 오류 형태 등이 거의 없음

- 특히 같은 언어를 가진 북한 요원의 댓글은 한국인과의 차이를 더욱 구분하기 어렵게 만들며,[6] 북한은 이를 적극적으로 활용, 언어적 댓글무기를 통해 커뮤니티, 인플루언서 SNS를 매개로한 영향력 공작의 효과를 극대화

○ 북한이 피싱메일 제작 및 공격대상 식별, 취약점 들을 정교하게 학습시킨 생성형 AI를 이용하게 될 경우, '인간-기계 협업(human-machine teaming)' 방식을 통해 상대적 약점이었던 공격인원의 부족마저도 해소, 영향공작의 위력을 배가시킬 전망

○ 더 나아가, 최근 북한은 노동당 통일전선부와 정찰총국 등을 중심으로 기존의 위압적인 체제 선전선동 방식을 좀더 세련되고 부드러운 접근으로 전환하고 있어 경각심이 요구됨

- 유튜브, 틱톡, 웨이보 등 글로벌 플랫폼에 자체 사이버 인플루언서를 활용한 콘텐츠를 업로드하는 방식으로, 유튜버 '유미', '송아' 등이 대표적
- 이들 영상은 영어, 중국어, 러시아어 등의 자막을 통해 평화롭게 일상을 즐기는 북한 젊은이의 모습을 구현하고 있으며 '정상국가'와 같은 북한사회의 이미지를 강조
- 최근 외국인 관광객이 직접 찍어 업로드 한 것으로 보이는 북한의 관광지와 친근한 풍경이 담긴 숏폼 영상들도 등장하고 있으며, 시청자로 하

6) 김은영, "북한의 사이버상 영향력공작 현황", 『이슈브리핑』 제18호, (2023. 12. 13.), p. 9.

여금, 북한사회에 대한 호감도 증가와 서구언론을 통해 접했던 사실정보를 오히려 불신하는 효과를 기대

○ 이에 대한 대응 방향을 살펴보면, 美국가정보장실(ODNI) 산하의 '영향력 공작대응센터(FMIC)'와 같이 영향력 공작의 징후, 탐지·경고 및 평가 역할을 주도할 조직체계 신설 및 기능별 임무 수행

- (임무 관리) 영향력 공작 관련 각 기관의 정보 수요 관리 및 수집정보 통합
- (분석 통합) 수집된 정보를 분석하여 정례적 동향 보고서를 생산·공유
- (대외 협력) 사이버인프라보안청, 등 기타 정부기관 및 국제 파트너들과 교류 확대

○ 동 센터에서는 행동분석 측면에서 영향공작의 메커니즘에 대한 실증적 연구도 지원

- 신념 변경, 투표 행동 변경, 정치적 폭력 조장 등 정치적 영향공작의 다양한 효과들이 언급되고는 있으나 파편적으로 이루어지고 있으며, 행동 변화의 단계별, 분야별 확신 강도별 의미를 담고 있지 못하여, 영향공작의 위협 우선순위를 정하고, 문제가 호전되는지 악화되는지 판단하고, 증거 기반 솔루션을 개발하는 것이 어려움

○ 최근 자유민주주의 진영을 중심으로 허위정보의 단속과 영향공작 차단을 위해 보다 능동적인 제도적 정비가 이루어지고 있음을 고려, 선거 위협 등 '사활적 문제'에 한해 외국인 간첩법과 사이버 허위정보 확산 금지법 등 포괄적이고 종합적인 대책 논의가 필요

- 미국 국토안보부의 경우, 선거에 대한 개입을 자유민주주의국가를 지

탱하는 제도적 '핵심 기반(critical infrastructure)'을 침해하는 위협행위로 규정하여 강력히 대응

- 캐나다 공공안전부는 '보안정보부법(CSIS)'을 개정하여 영향력 공작 혐의자에 대한 정보기관의 민감정보 수집·공유 허용 및 영장발부 범위를 확대 중
- EU 또한 최근 러시아發 허위정보의 확산을 막기위해 '메타(Meta)'와 같은 빅테크 플랫폼 기업에 정치광고·콘텐츠 관리 규정을 엄격히 하는 의무조치를 부과한 바 있음

※ 중요 국가안보 관련 사안의 경우 SNS 데이터에 대한 접근성을 높여 자체 모니터링 시스템을 확보할 수 있도록 권한을 허용하는 방안도 고려할 필요

○ 이른바 '허위정보의 위험층위' 기준(ex. '허용불가한', '고위험', '최소한' 등) 원칙, 규정을 마련, 위중한 가짜뉴스에 대해서는 징벌적 손해배상제도를 적용하는 등, 능동적 조치 시행

○ 사회적 '정보 리터러시(Information Literacy)' 강화를 위한 프로그램 마련 및 적극적인 대국민 소통을 통해 자유민주주의의 가치와 사회적 공익 수호를 위한 사회적 합의 거양

○ 투명성·개방성·자유와 같은 핵심 민주적 가치를 추구하는 시민사회에 자원과 도구를 전달, 악의적 정보공작에 대한 회복탄력성 증진

3. 대북 사이버 제재 공조체계 구축

○ 최근 국제사회와 우리나라가 대북 사이버 경제제재를 검토하고 있으나, 여전히 효과에는 의구심이 제기되고 있는 바, 사이버제재의 실효성을 담보할 구체적 방안 모색이 필요

- 現대북제재의 빈틈과 취약점이 되고 있는 사이버 공간에서의 제재 위반 행위 모니터링, 불법적 기술이전, IT노동력 수출, 자금 조달 등 北의 제재 우회와 초국적 사이버 불법행위 억제를 위한 국제사회의 경각심 제고, 책임귀속, 수출통제 금융기관 접근 차단 등의 세부 실천방안의 구체화가 요구됨

○ 특히, 유엔 안보리 대북 제재 위원회 전문가 패널이 러시아의 반대와 중국의 기권으로 활동 연장에 실패하여 2024년 4월 30일로 활동 종료되어 대북 제재 이행을 감시할 수 있는 대안적 차원의 접근과 활동 분야를 복원하고 지원할 필요한 상황

○ 최근 대북 사이버 제재 시도와 한계에 대해서 살펴보면, 우리 정부는 2023년 2월 10일 북한의 불법 사이버 활동에 대응하기 위해 첫 대북 독자제재를 단행한 바 있음

- 해킹·가상자산 탈취 등 불법 사이버 활동을 벌였거나 관련 프로그램 개발 및 전문인력 양성에 관여한 혐의를 갖는 개인이나 기관 7곳을 독자제재 대상으로 지정

※ 박진혁, 조명래, 송림, 오충성, 심현섭 등 북한인 4명과 조선엑스포합영회

사, 라자루스 그룹, 블루노로프, 안다리엘, 기술정찰국, 110호 연구소, 지휘자동화대학(미림대학) 등

- 미국과 유럽연합 등도 북한의 불법 사이버 활동을 주도하고 있는 개인과 단체에 대한 사이버 경제제재를 단행하고 있으며, 특히 미국은 국가안보, 외교정책 및 경제에 비정상적인 위협을 야기하는 악의적 사이버 활동의 경우 제재(sanction)를 부과

  ※ 2015년 오바마 대통령이 발령한 행정명령 제13694호에 근거하여 사이버 경제제재를 단행한 바 있으며, 서방의 정보기관 등과 악의적 국가배후 사이버 활동 등에 대해 공동으로 비난 성명이나 보안 권고문을 발표

- 국가정보원 역시 2023년 2월 10일 미국의 국가안보국(NSA)·연방수사국(FBI) 등과 함께 북한의 사이버공격 위협 실태를 알리고 이를 예방하기 위한 보안 권고문을 발표하였으나 실효성 담보를 위한 국제공조와 세부 조치사항에 대한 논의가 필요[7)]

- 이에 대한 대응방향을 모색하는 차원에서 사이버 제재 실효성을 높이기 위해서는 미국 등 서방의 사이버안보 관련 기관들과의 협력하에 비난, 권고, 지명과 책임귀속, 수출통제와 금융기관 접근 차단 등의 조치를 실행할 필요

7) 김성훈, "北, 세계 각국 상대로 해킹" 국정원·FBI 등 공동 경고, 매일경제(2023. 2. 10), https://www.mk.co.kr/news/politics/10638613

- UN GGE, OEWG 등 국제사회의 책임귀속 논의에 적극 참여하고, 탈린 매뉴얼 개정을 통해 책임귀속을 위한 기술적 법제적 기준을 구체화하는데 적극 참여
- 국내외 증거법과는 차별화된 책임귀속 기준을 정립하고 그에 따라 사이버제제 등을 부과할 수 있도록 사이버안보기본법(안) 등을 통해 이에 대한 법적 뒷받침을 마련
- 사이버 제재를 단행하는 경우 제재 대상 개인이나 기관에 접근하지 못하도록 이들과 거래하는 제3국 금융기관(특히 중국)에 대한 제재를 부과할 수도 있도록 조치

○ 특히, 제재 대상인 북한 해커 및 이들과 연계된 북한 기관이 보유한 자산에 대한 동결 및 몰수 조치를 강행할 수 있는 입법적 조치를 고려할 필요가 있으며, 러-우 전쟁 이후 미국의 대러 경제제재 및 해외 국영자산 몰수의 사례를 참고할 필요

- 2024년 4월 23일 미 의회의 「우크라이나 경제 번영 및 기회 재건 법안(the Rebuilding Economic Prosperity and Opportunity for Ukrainians Act : REPO)」을 통과시켰고, 우크라이나 지원 내용 뿐만 아니라 러시아 국영자산의 몰수 관련 규정도 명시
- 미국의 관할권에 있는 침략국 러시아의 국영 자산의 전부 또는 일부, 그리고 그러한 자산의 이자 혹은 이해관계 등을 압류(seize), 몰수(confiscate), 양도(transfer) 또는 귀속(vest)시킬 수 있도록 규정
- 위 법을 참고하여 북한 해커가 보유하고 있는 암호화폐 및 금융계좌에 대해 동결 및 몰수하여 북한 인권 개선 혹은 탈북자 지원에 사용할 수 있도록 하는 입법을 통해 사이버 제재의 실효성을 강구할 필요

○ 사이버 제재 대상 북한 해커에 대한 법집행 활동 강화 방안 모색

- 미국은 2023년 3월 2일 발표한 「국가사이버안보전략(National Cybersecurity Strategy)」을 통해 정부 시스템의 보안 강화, 민간 기업 특히 주요 기반시설 소유자와 운영자의 시스템 보안 지원은 물론, 외교, 정보활동, 경제제재 부과, 법집행, 사이버위협에 대한 와해 활동(disruptive actions)을 수행하는 것으로 규정한 바 있음
- 해커 조직의 와해와 해체는 곧 디지털 생태계를 교란하여 디지털 경제와 공급망을 위협하거나 신기술을 탈취하는 사이버범죄자를 소탕하는 강력한 실천이라는 인식을 내포

○ 미국의 국제 해커 조직 와해와 해체 활동에 대해 우리 정보기관이나 법집행 기관의 적극적 참여를 보장할 수 있도록 제도 정비

- 북한 해커를 포함한 국제 해커 조직 및 단체에 대해 책임귀속을 실행할 수 있는 기술적 정보의를 수집·제공하고, 미국 정보기관 및 법집행기관들과 함께 북한 해커를 포함한 국제 해커 조직 및 단체를 직접 찾아 처벌 기소할 수 있는 활동 강화

※ 2021년 6월 16일 인터폴(IGCI)의 지원 하에 한국 및 미국의 법 집행기관은 우쿠라이나 경찰과 협력하여 랜섬웨어 범죄단체인 크롭(Clop)그룹의 용의자들을 체포한바 있으며 구속된 6명의 용의자들은 한국과 미국의 기업들에게 랜섬웨어 공격을 감행하여 총 5억 달러에 이르는 대가(몸값)을 받은 것으로 알려짐[8)]

8) https://therecord.media/ukrainian-police-arrest-clop-ransomware-members-seize-

- 나아가 북한의 랜섬웨어 공격, 암호화폐거래소와 금융기관에 대한 사이버공격 등 외화벌이와 자금 탈취 관련 불법 사이버 활동 차단을 위한 한미 간 공조를 강화

○ 국제 '자금세탁방지기구(FATF)와의 협력 강화로 글로벌 규제 표준 수립 및 국제 사이버 보안 이니셔티브 확보

※ FATF는 "[가상 자산] 및 [가상 자산 서비스 제공자]에 대한 FATF의 기준 채택 이후 4년이 경과했지만, 일부 관할 구역만이 규제를 도입했으며, 전 세계적으로 이를 이행하는 것은 상대적으로 미흡하고 대부분의 다른 금융 부문보다 뒤처져 있음을 지적[9)]

- 각국의 암호화폐 거래소에 대한 AML(자금세탁방지) 및 KYC(고객신원확인) 규제 강화 및 통일된 규제 체계 마련

server-infrastructure/

9) Alex O'Neill, Upholding North Korea Sanctions in the Age of Decentralised Finance, RUSI Occasional Paper (런던: Royal United Services Institute for Defence and Security Studies, 2024), 30, https://static.rusi.org/north-korea-sanctions-and-cryptomixers-op-march-2024.pdf.

4. 북한사회의 디지털 억압 실태 개선

○ 그간 북한 사회의 정보화에 노력해왔던 김정은 체제는 다른 권위주의 국가의 지도자와 마찬가지로 정보 접근성의 확대 및 효율화와 정보 통제라는 양 가치 사이에서 선택을 요구받고 있으며 최근 정치 안정성을 위한 정보 차단 및 통제에 주안하고 있는 추세

- 최근 북한의 연이은 사회통제 악법(반동사상문화배격법(2020.12), 청년교양보장법(2021.9), 평양문화어보호법(2022.12), 국가비밀보호법(2023.2)) 제정은 정보 유입 문제와 관련한 북한 정권의 상당한 우려를 방증

○ 북한의 앙시앙 레짐(절대왕정체제)를 깨기 위해서는 다양한 접근을 통한 외부 정보 유입이 필수 조건이나 북한의 정권 안보(regime security) 차원의 사활적인 방비 노력을 강화 중

- 인터넷 전면 차단, 미승인 프로그램 사용 금지 등 북한의 정보차단 수위는 다른 어떤 전체주의 국가와 비교해도 월등히 높은 상황

○ 지난 2023년 11월 29일 서울에서 개최된 북한인권 개선관련 국제회의에서는 이 같은 북한 사회의 디지털 억압 실태에 대해 심층적으로 논의한 한 바 있으나 실천방안에 한계

- 폐쇄적인 북한 사회의 디지털 억압을 해소하고 인권을 개선하기 위한 기존의 노력들은 주로 전단 살포 등 물리적 수단에 의존, 효과성에 한계를 노정
- 북한사회의 올바른 정보 유입과 인권 개선을 위한 차세대 통신체계 등

비(非)네트워크 수단과 차별화된 디지털 자유화 방안의 가능성과 파급력 탐색이 필요

○ 최근 우회 프로그램 수요 증가 및 그로 인한 다각화로 2022년 기준 10여 종의 우회 프로그램이 통용중인 것으로 추정

- 주요 대학 및 내각 정보산업성 산하 연구소·센터 혹은 주요 대학 소속 엘리트를 중심으로 개발 및 유통
- '비둘기'(PC용 인증 회피 프로그램으로 '비둘기'의 기본형인 '참매'도 상용), '미궁'('열람리력' 저장 스크린샷 삭제), '3차원 세계'(특정 파일 은폐) 등 다양
- 프로그램 개발 목적이 정보자유화 보다는 단순한 수익 창출로 판단되며, 따라서 적발시 처벌 수위도 외부 정보 유입 관련 처벌 대비 경형(輕刑) 예상
- '가락지'의 경우 조선 컴퓨터센터 산하 붉은별 연구소에서 개발된 것으로 추측되며 평양 대학생 약 10%가 활용중이고 보위부·안전부 등 정부 기관 종사자 포함 사회 전반 확산

○ 최근, 북한 사회의 디지털 억압 실태를 살펴보면, 북한은 IT 거버넌스에 있어 중앙집중화를 추구, 디지털 권위주의(Digital Authori- tarianism)의 효과적 도구로써 통제와 감시의 기능으로 활용하는 방안을 적극 모색 중

- 권력 유지를 위해 방어적 체제 수호 전략 아래 사회적 제한과 순응을 강요하고 디지털 정보 흐름을 차단하여 북한 주민의 의식과 담론 형성을 왜곡, 권위주의 통제의 범위와 영향력을 확대 중
- 북한 정권이 이동통신망 구축 초기 과정에서부터 가장 우선적으로 고려했던 사항은 통화와 데이터 전송에 대한 당국의 모니터링 가능 여부였음

※ 북한 전문 美 보도 매체인 38North가 2000년대 후반 당시 북한 체신성과 이집트 오라스콤과의 협의 내용을 입수하여 공개한 자료에 따르면, 북한은 오라스콤측에 내국인이 사용하는 통신망과 외국인이 사용하는 통신망을 분리하고, 고위층 전용통신망을 별도로 구축할 것을 요청한 바 있음[10)]

○ 현재 북한은 내부에서는 외부세계와 연결되지 않은 내부망 인트라넷인 '광명망'을 도입하여 망 내에서만 자료를 검색하거나 이메일을 주고 받고 있음

- 인터넷 접속을 허용한 극소수의 해외 및 대남사업 기관원(해커 포함)들이나 IT 전공 학업자들만 중·러의 IP 주소를 통해 월드와이드웹(WWW)에 접속 가능[11)]
- 해외 동향 및 정보 수집, 해외 선전 계정 관리, IT 전문가 육성 등을 위해서 최소한의 인터넷 사용이 불가피하지만, 이마저도 전 과정이 기록·감시되기 때문에 자유로운 사용에는 제약
- 휴대전화 역시 인트라넷을 통한 사용만 가능하고, 국제통화와 인터넷 접속은 불가한 상황

※ 조선컴퓨터센터가 자체 개발한 '붉은별' 운영체제(OS) 아래 와이파이 모듈을 제거한 후 휴대전화를 보급하기 때문에 북한에서 생산한 휴대전화는 와이파이를 통한 인터넷 접속이 불가. 일부 와이파이 모듈이 내장된 휴대전

10) https://www.38north.org/2019/07/mwilliams072219

11) 싱가포르에 기반을 둔 데이터 분석 기관 '데이터리포탈(DataReportal)'이 발표한 '디지털 2024 글로벌 보고서'에 따르면 북한 인구의 99.9% 이상이 인터넷 비연결 상태로 파악.
세부내용은 https://datareportal.com/reports/digital-2024-global-overview-report 참조.

화의 경우에도 '미래'라는 앱을 통해 인트라넷에만 접속 가능

○ 최근 정보 공유를 매개로 개인간 정보교류가 급격하게 증가하자 북한 당국은 모든 정보통신기기에 정부의 승인받지 파일의 열람을 제한하는 조치를 실시

- 과거 이집트 오라스콤과의 합작회사인 '고려링크'를 통한 3세대 통신망 도입 초기에는 북한의 스마트폰으로도 K-POP을 듣거나 한국 드라마와 영화를 시청하고 촬영한 사진과 동영상을 블루투스 기능으로 다른 휴대전화로 전송할 수 있었음

○ 그러나, 이제 정부서명이 없는 앱 설치나 중국에서 밀반입된 파일 열람은 불가능하며 '붉은별' 운영체제의 서명 확인 소프트웨어(signature-checking software)가 서명 여부를 확인하고 서명이 없으면 제거시키거나 해당 장치에 의해 생성된 파일이 아닌 여타 모든 파일은 열리지 않도록 설정되었으며, 사용자가 임의 시스템 변경·제거 시도 시 셧다운되도록 설정

- 소프트웨어 차원에서는 모든 정보통신 기기에 사용자의 사용기록을 남기고 불규칙적 간격으로 스크린 화면을 캡쳐하여 저장하는 '열람추적기(Trace Viewer)' 프로그램도 설치, 중층적인 상시추적체계를 통해 사용자로 하여금 단속의 빌미가 될 수 있는 파일 생성이나 열람을 스스로 제한시키는 자기검열적 태도를 확산 중

○ 이에 대한 대응방향을 살펴보면, '북한인권법 제301조'에 기반하여 북한 정보통제 대응 기술개발을 위한 다양한 프로젝트를 지원 중인 미국의 사

례를 참조, 북한 사회의 디지털 억압 개선을 위한 재정지원 기반 마련

- 미 정부는 인터넷 접근성 향상 및 기술의 연구·개발·실행·지원기관인 '개방기술기금'을 '국제방송처' 관할기관으로 두어 정보 자유화 연구와 함께 디지털 검열, 감시, 인터넷 차단 대응 기술개발 및 지원을 실행 중

○ 북한 사회 내의 디지털 정보 활용 능력은 여전히 미약한바, 북한 내부의 정보화(네트워크화) 수준과 외부의 기술적 침습도를 종합 고려한 신기술 적용 가능성 검토 필요

- 현재 북한의 내외망분리, 별도운영체제, 전자서명체계 등을 초월하거나 우회한 침습적 기술력 확보가 가능한지에 대해서는 별도의 기술공학적 검토가 필요
- 역설적으로 현재 라디오, 대북방송, 대북전단, 개별포섭(co-optation) 방식 등을 활용한 아날로그적 접근의 유용성도 여전히 존재함을 고려할 필요가 있으며, 특히 저개발 국가나 절연된 국가에 네트워크 기반 기술적 접근이 실효적이지 않을 수 있기 때문

○ 정보통신 매체를 활용하려 할 경우, 외국산 정보통신기기 비합법적 보급을 통한 외국공관 주변 와이파이 접속, 중북 국경지대에서 북한산 외 미등록 기기(중국폰, 한국산 중고폰[12] 등)를 통한 중국 네트워크망 사용 등 고

12) 북한의 이동통신망은 주파수 2100㎒의 광대역 코드다중분할접속(WCDMA) 방식을 사용하며 SKT나 KT도 같은 방식이어서 한국산 스마트폰도 대부분 유심만 갈아 끼우면 북한에서 사용 가능

려 가능[13)]

- 장기적 차원에서 북한 통제 우회 기술개발, 위성 인터넷 도입을 목표로 한 프로젝트 추진
  - 국경 전파방해 차단 및 국가망 접속 인증체계 교란기술 개발, Space-X 사의 직접통신(D2D) 위성기술 활용 방식의 적용 방안 등 차세대 네트워크 신기술을 활용한 혁신적 돌파구 모색

- 지난 3월 스페이스엑스사의 D2D 위성기술 공개로 대북 위성 인터넷 서비스 도입 위한 1차 여건 조성
  - 대북 제재 및 국제사회 통신규정, 기술적 장애요인 등 공급 제한 제반 요인이 산재하나 위성인터넷의 가장 큰 제한요건이었던 위성안테나 설치 및 별도 장비 반입 불요
  - 북한 정권의 첨단 신호 감지·식별·차단 기술을 활용한 실시간 전파추적 및 네트워크 침투 등 방해공작 우려

- 非네트워크적 디지털 혁신기술 개발 검토
  - 북한 정권의 디지털 통제 수준·범위·강도는 중국·이란 등 여타 독재국가 대비 매우 심각하여, 기존 개발된 온라인 검열 완화·우회기술 사용 불가

13) . 다만, 이런 현상과 확산 가능성에 대비해 북한 당국도 운영체제 업데이트(붉은별 4.0), 전파탐지장비 등을 도입해 적극적으로 대비에 나서는 양상

→ 이란·중국 포함 대부분 국가는 특정 웹사이트 접속 차단, 키워드 검열, 온라인 감시 등 부분적인 통제 수준

- 4G 스마크기기 상용화 등 북한 정보통신 환경 변화가 예상되는 바, 다양한 진화된 디지털 기술에 대한 활용방안을 모색할 적기라 판단
- 오프라인용 생성형 인공지능 앱의 경우, 실현 가능성 타진 및 최적 환경 분석을 위한 파일럿 AI모델 개발 完

○ 국제사회 협력 확대

- 2022 미 국방수권법에 북한의 '억압적 안보환경에 대한 대응 전략' 수립을 의무화하는 '오토 웜비어 북한 검열 및 감시법'이 포함되는 등 미 정부 및 의회는 북한 사회 혁신을 위한 신기술 활용전략에 적극적
- 미국은 재무부는 이란의 디지털 억압 상황 개선 및 시민들에게 자유로운 인터넷 활용을 보장하기 위해 對이란 제재 규정을 일부 완화 후, 스타링크社가 위성 인터넷 서비스를 제공하도록 제도 여건 마련한 바 있음('22. 9)[14)]

14) 중국 인터넷서비스 활용도 제고 등 기타 대북 정보유입 사이버 기술 관련 사항은 김민정의 연구, '대북 정보 유입 활성화를 위한 기술 혁신 방안,' '직접통신(D2D) 위성기술을 활용한 대북 정보 유입 방안-스타링크 서비스 도입을 중심으로' 등 참조

5. 북한 사회의 디지털 환경 실태 진단 및 활용방안 탐색

○ 북한 내부의 디지털 환경 실태에 대한 면밀한 분석은 북한의 사이버 취약점 판단과 장기적 관점에서 북한 사회의 개방, 개발 검토 시 우선적으로 정밀한 검토가 필요한 사안임

○ 특히, 급변사태, 비핵화 진전을 고려한 북한 개방 시나리오는 언제든지 발생할 수 있으므로 이 같은 국면 전환 하에서 효과적인 대북 교류, 사업을 위한 로드맵의 준비가 필요

- 단순한 일방적 북한 정보인프라 개선 지원 구상이 아닌, 호혜성에 기반한 접근을 고려한 접근으로서 북한 내 정보 디지털화 방향 및 우선순위 탐색이 요구됨

○ 나아가, 공세적 관점에서 우리의 대북 사이버 역량을 강화하기 위해서는 북한 내부의 디지털 환경 실태에 대한 면밀한 분석과 활용 방안에 대한 연구가 병행되어야 함

- 북한도 제한적이긴 하나, 디지털 기기와 서비스를 경험하며 인터넷 자유도에 대한 인식을 가지고 있는 바, 전면차단의 불편성을 강조하여 정권불만을 유도할 수 있는 방안 탐색

○ 북한 사회의 디지털 활용 실태를 살펴보면, 인터넷에 자유롭게 접속할 수 없는 북한에서 스마트폰과 태블릿PC용 애플리케이션(앱)인 '나의 길

동무'는 북한 주민들 사이에서 인기[15]

- 한편 평양 주민의 휴대전화 보급률은 71.2%, 접경지역과 비(非)접경지역'에서는 각각 31.1%와 36.0%로 조사되었으며, 컴퓨터 보유율은 평양지역, 접경지역, 비접경지역이 각각 58.3%, 16.4%, 16.9%를 기록한 바 있음[16]
- 김정은 집권 이후 휴대전화 36.4%, 컴퓨터 19.6% 등 정보기기의 전반적 확산 현상이 나타나고 있는 것으로 조사됨[17]

○ 비록 북한 휴대전화 이용 비율이 북한 전체 인구의 약 30%로 추정되지만 평양, 평성, 청진 등 대도시에 집중되어 있고 소득수준에 따른 비대칭 현상 또한 관찰됨[18]

- 한편 북한에도 2015년 이후 '옥류'를 비롯하여 '만물상', '은파산', '앞날' 등 전자상거래(온라인쇼핑몰)이 등장하여 400여 개의 기업들이 450종류, 6만여 점의 상품을 판매하고 있다는 주장도 존재[19]
- 이러한 전자상거래의 발전은 PC와 휴대전화 사용자 급증, 전자결제 카드 이용 확대, 오토바이, 택배차량 등 배달 서비스의 확대에 따른 것이

15) 최아영, "북한 주민들도 스마트폰 사용?…'최고 인기앱' 등극했다는 이것", 매일경제(2023. 11. 12), https://www.mk.co.kr/news/politics/10872501

16) 하채림, "평양 휴대전화 보급률 71%…접경지는 31% 수준", 연합뉴스(2023. 9. 5), https://www.yna.co.kr/view/AKR20230905062000504

17) 통일부, 「북한 경제·사회 실태 인식보고서」, 2024. 2., p.199.

18) 통일부, 앞의 보고서, p. 204.

19) 김진무, "6. 북한의 시장과 정권: 시장의 종류: 공식시장", 2024. 3. 7., https://blog.naver.com/jmkim0778/223376224769

라고 주장[20)]

○ 또한, 북한은 전자상거래 사이트 '만물상'을 통해 자력갱생'의 상징 중 하나로 '나래' 위생자기(위생도기)를 판매하고 이 자기를 유튜브 채널을 통해 선전한 바 있음

- 이러한 점에서 볼 때 북한 일부 특권 주민들이 전자상거래를 통해 편의성을 누리고 있는 것으로 추정되는바, 이에 대한 차단은 북한 정권에 대한 불만으로 작용할 가능성 존재

○ 한편, 북한 개발의 경우 북한이 보유하고 있는 도로, 철도, 교량, 지형, 통계, 채굴도, 구조물 등 각종 데이터와 자료에 기초

- 이들 데이터나 기록은 주로 종이문서 기반으로 보존중이어서, 유실과 변형, 삭제의 위험에 노출
- 우리 정부는 지난 2006년 6월, 북한 단천 지역 3개 광산을 개발하기로 한 사업(검덕, 용한, 대흥)을 추진한 바 있음

※ '남북 경공업 및 지하자원개발 협력에 관한 협의서'에 기초하여 마그네슘, 연, 아연의 개발·생산을 위해 30년의 중장기 전략을 수립한 바 있으며 이후 2007년에 북한은 위 광산에 대한 지질도 등 자료를 제공하고 남북 공동조사단이 현지조사를 완료

- 사업에 참가한 우리 측 관계자들은 북한은 정보통신 인프라가 미흡하여 광산 관련 자료를 수기로 도면을 그려서 제출하는 등 자료 제공에

20) 김진무(2024. 3. 7.).

상당한 어려움이 있었음을 언급

※ 당시 언론 보도와 달리 자료를 주지 않으려고 한 것이 아니라 기술적으로 자료 제공에 어려움이 있었던 것으로 추정

○ 이에 대한 대응 방향을 모색하는 차원에서 공세적 관점에서 탈북자를 중심으로 우리의 대북 사이버 역량을 강화하기 위해 북한 사회 계층별 디지털 환경 실태에 대한 조사 프로젝트 및 활용 인식 조사 연구 수행 필요

○ 미국이 추진하고 있는 AI칩에 대한 수출통제는 물론 관련 소프트웨어에 대한 수출 차단 등에 협력하여 북한의 인공지능 기술 개발을 저지하고, 북한 주민들의 디지털 활동의 확대를 저지하여 불만을 고조시킬 필요

○ 이익공유에 기초하여 북한 인프라·자원 등 개발 및 관련 자료의 디지털화 기반 검토

- 기존 북한 개발은 남한의 일방적인 지원에 기초한 측면이 비판적으로 제기되었는 바, 북한 개발에 따른 이익을 남북이 공유하는 방향으로 추진할 필요
- 따라서 향후 북한 개발이 추진되는 경우(특히 북한 자원개발) 그 이익을 남북이 균분할 수 있도록 제도화할 필요

○ 남북교류 협력이 중단된 지금, 급변사태나 비핵화의 모든 가능성을 열어두고 북한의 자료와 데이터에 대한 디지털화를 위한 기반 조성을 선제적으로 준비할 필요성도 존재

- 장기적 관점에서 남북관계의 분위기 전환으로 북한 개발이 진행되는

경우의 모든 시나리오를 상정, 우리의 이익을 실현하기 위해 북한 경제 및 산업은 물론 공장과 기업 등에 대한 데이터의 수집과 관리 체계 구축 필요

- 통일부 북한자료센터를 확대 개편하여 입수된 북한의 각종 데이터와 자료의 디지털 전환 사업 추진이나 통일연구원에 북한 디지털전환센터를 설립하여 북한의 광산이나 기반시설 관련 자료와 데이터의 디지털 전환에 대한 기초연구를 수행하도록 지원

  ※ 최근 북한 과학백과사전출판사가 발간한 경제연구 2020년 3호(2020. 12. 2)는 '지식자원, 정보자원의 관리는 생산 선행공정의 중요한 사업'이라는 글을 게시한 바 있음[21)]

- 따라서 북한의 공장이나 기업 등에서 축적되고 있는 정보자원(데이터)에 대해 제3국의 데이터 중개 혹은 거래 업체 등을 통해 접근하여 확보하고 축적·분석함으로써 향후 우리의 이익공유 개발사업에 이용할 필요

21) 이 글은 북한 노동당이 모든 공장, 기업들에서 지식자원, 정보자원을 중요한 생산자원으로 틀어쥐고 지식과 정보의 힘으로 경제를 발전시킬 것을 요구하고 있다"고 주장하며, 오늘날 생산에서 정보와 지식이 역할이 더욱 중요해졌으며, 모든 생산과정이 정보화로 전환되고 있다고 강조하였음.

제8장

사이버 안보 동맹협력 및 소다자 협력

송 태 은 | 국립외교원 국제안보통일연구부 조교수

1. 한국의 사이버 안보 역량과 협력 대상 선호도 증가
2. 한·미 동맹 협력 의제와 전략
3. 한·미·일 및 한·일 사이버 안보 협력
4. 인태지역 소다자 그룹과의 사이버 안보 협력
5. 유럽 및 NATO와의 사이버 안보 협력
6. 결론

제8장

사이버 안보 동맹협력 및 소다자 협력

송 태 은 | 국립외교원 국제안보통일연구부 조교수

배경과 구성

- 최근 한국은 사이버 안보 분야에서 동맹 미국뿐만 아니라 유럽과 인태 지역 우호국들과 다양한 국제협력을 도모하고 있으며, 협력의 수준 역시 실질적으로 확장, 강화되고 있음
- 이처럼 사이버 안보 분야에서 한국이 주요 협력 파트너로 주목받기 시작한 배경에는 한국의 사이버 안보 역량(특히 기술적 측면) 증가가 주된 요인으로 작용함
- 한국의 사이버 기술 경쟁력과 협력 대상국으로서의 국제적 선호도가 증가하고 있음에도 불구하고 사이버 안보 분야에서 나타나는 인력·자원·예산 부족은 글로벌 협력의 증대를 가로막는 걸림돌이 될 수 있음
- 글로벌 중추 국가의 위상과 역할을 지향하는 한국이 사이버 안보 분야에서의 국제협력을 통해 어떻게 직접적이고 가시적인 실질적 성과를 거두며 우리의 안보 이익을 증진시킬 수 있는지, 그리고 한국에 대한 국제사회의 다양한 요청과 기대에 부응할 것인지 동맹과 소다자 협력의 차원에서 모색하고 협력의제의 우선순위를 가려낼 필요가 있음

- 제8장의 구성은 아래와 같이 다섯 가지 항목을 중심으로 함

  1. 한국의 사이버 안보 역량과 협력 대상 선호도 증가
  2. 한·미 동맹 협력 의제와 전략
  3. 한·미·일 및 한·일 사이버 안보 협력
  4. 인태지역 소다자 그룹과의 사이버 안보 협력
  5. 유럽 및 NATO와의 사이버 안보 협력
  6. 결론

1. 한국의 사이버 안보 역량과 협력 대상 선호도 증가

○ 최근 우리 정부는 다양한 군사안보 분야 중 특히 사이버 안보 분야에서 동맹 미국뿐 아니라 유럽과 인태지역 우호국들과 다양한 국제협력을 도모하고 있고 협력의 수준이 실질적으로 확장, 강화되고 있음.

○ 호주, 일본, 인도, 뉴질랜드와 같은 인태 주요국들과 영국, 독일, 네덜란드 등 유럽국들과 동아시아 개발도상국들이 사이버 안보 분야에서 한국을 주요 협력 파트너로 인식하는 것은 국제사회에 알려져 있는 한국의 사이버 안보 역량(특히 기술적 측면)이 주요 요인임.

- 로위연구소(Lowy Institute)가 측정한 2021-2022년 각국의 사이버 역량(Cyber Capabilities) 순위에서 4위(북한 7위), MIT Technology Review가 측정한 Cyber Defense Index(2022)에서 3위(북한은 20위권에 들어있지 않음), 하버드대 벨퍼센터(Belfer Center)가 측정한 2022-2023년 국가사이

버전력지수(National Cyber Power Index) 종합지수에서는 7위(북한은 10위권 밖)를 기록하여 일관성 있게 높은 평가를 받고 있음.

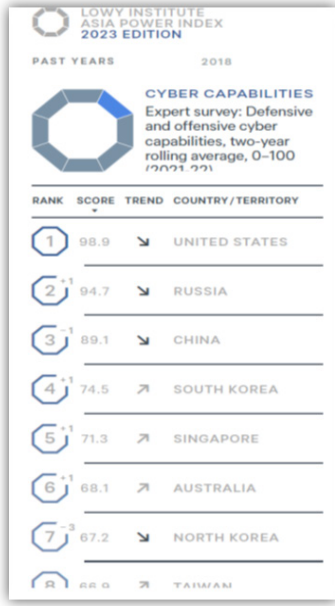
- 사이버 역량 평가 기준이나 측정 방식에 따라서 한국의 사이버 역량의 국제적 순위가 조금씩 다름. 벨퍼센터의 NCPI의 경우 국가의 사이버 역량 자체에 더하여 그러한 역량을 사용할 '의도(intent)'가 가중치로 반영되어 계산이 되는데, 한국은 사이버 공격 역량을 보유하고 있으나 그러한 공격력을 사용할 의도가 낮아 종합지수에서 랭킹이 다소 낮게 나옴. 러시아와 중국을 제외할 경우 민주주의 국가 중 한국보다 사이버 역량이 크면서 그러한 역량을 사용할 의도가 큰 국가는 미국과 영국이 유일함.

〈그림 8-1〉

Table 1. NCPI 2022: Top 10 Most Comprehensive Cyber Powers

Rank	2022
1	US
2	China
3	Russia
4	UK
5	Australia
6	Netherlands
7	ROK
8	Vietnam
9	France
10	Iran

〈그림 8-2〉



- 한국은 네덜란드가 주관하는 국제사이버 대회인 CyberNet에서 2022년과 2023년 연속 우승했고, 한국이 영국과 연합팀을 구성하여 처음

참가한, 17개국이 참가한 2024년 2월 개최된 제3회 국제 사이버훈련(Defence Cyber Marvel, DCM)에서 우승하는 등 기술 차원에서의 세계적 실력이 반복적으로 입증되고 있음.

- 특히 2024년 2월 정부가 발표한 『국가사이버안보전략』과 9월 발표한 『국가사이버안보기본계획』이 공표하고 있는 ▲공세적 사이버 방어 대응, ▲글로벌 사이버 공조 체계 구축, ▲국가 핵심 인프라 사이버 복원력 강화 및 ▲신기술 경쟁 우위의 확보는 모두 동맹 미국 및 인태지역 주요국, 유럽과 긴밀한 전방위적 공조 체제와 상시 협력관계를 요구하고 있음.

- 정부가 2024년 9월 발표한 기본계획은 국제협력에 있어서 한국이 어떤 의제에 초점을 둘 것인지 가이드라인을 제시하는 효과를 가지며 협력의 '상대'와 '분야'에 따라 우리가 추진할 사이버 안보 외교에 있어서도 세분화된, 치밀하고도 단계적인 정책 구상을 필요로 함.

- 한국이 보유한 사이버 기술이 우수함에도 불구하고 부족한 인력과 자원 및 예산은 사실상 우리의 글로벌 협력을 제한하고 있는 것이 현실이므로 우선순위와 집중분야에 대한 전략적 검토가 필요한 실정임.

- 이 연구는 글로벌 중추 국가의 위상과 역할을 지향하는 우리 정부가 사이버 안보 분야에서의 국제협력을 통해 어떻게 직접적이고 가시적인 실질적 성과를 거두며 우리의 안보 이익을 증진시킬 수 있는지, 그리고 우리에 대한 국제사회의 다양한 요청과 기대에 부응할 것인지 동맹과 소다자 협력의 차원에서 모색하고 협력의제의 우선순위를 가려내고자 함.

2. 한·미 동맹 협력 의제와 전략

한미 사이버 훈련 강화 및 인태지역에서의 시그니처 사이버 훈련 추진

- 2024년 1월 15-26일 한국의 사이버작전사령부(R.O.K. Cyber Operations Command)와 미국의 사이버사령부(U.S. Cyber Command)가 최초로 수행하고 성공적으로 완료한 '사이버 동맹 훈련(ROK-U.S. Cyber Alliance exercise)'은 한국이 훈련 전체를 기획하고 진행하는 등 한국의 사이버 기술과 훈련을 위한 시설 구비 등 전반적인 역량 부재 시에는 성공적 진행이 어려웠을 것임.
  - 한국의 사이버 작전 수행 역량이 양자 훈련을 통해 세밀한 부분에서의 한국의 사이버 기술 및 전력이 발휘된 것은 이번 한미 사이버 동맹 훈련이 최초였고, 미국도 한국의 실제 우수한 역량을 사실상 처음 확인한 의미가 있음.
  - 한국이 주도한 이번 훈련이 성공적으로 진행됨에 따라 양국은 2025년 초 미국 메릴랜드(Maryland)에서 제2차 사이버 동맹 훈련을 추진하기로 함.

- 한미는 2024년 8월 을지 자유의방패(Freedom Shield, UFS) 훈련에서 사이버 영역(domain)에서의 위기 발생 가능성을 염두에 둔 민관군이 모두 참여하는 훈련을 최초로 수행함.
  - 이번 UFS가 외부로부터의 사이버 위협이 물리적 공격과 결합되는 하이브리드전(hybrid warfare) 시나리오를 가정한 훈련을 포함함으로써 2024년 1월 한미 간 사이버 훈련이 별도의 독립 훈련으로 이뤄진 성과를 뛰어넘는 발전을 보여준 것임.

- 이러한 성과를 기반으로 향후 한미동맹의 다양한 정례 연합훈련인 키리졸브(Key Resolve) 훈련, 독수리(Foal Eagle) 훈련에도 사이버 훈련이 포함될 가능성이 높아짐.

○ 사이버 공간과 물리적 공간이 결합되는 현대와 미래의 초연결 전장 환경을 감안, 한미동맹의 연합 사이버 작전은 향후 지상·해상·공중뿐 아니라 우주작전과도 완전히 결합된 형태로 발전해야 하며, 이러한 훈련은 양국간의 우주협력 강화에도 기여할 것임.

○ 단 기존의 다양한 한미연합훈련에 사이버 훈련을 포함시킬 경우 이에 수반되는 예산과 전문 인력에 대한 부담요소가 있으므로 국가적 차원에서의 전폭적인 지원이 필요함.

○ 향후 한미 사이버 동맹 훈련을 확대시켜 인태지역에서의 시그너쳐 훈련인 '인태 사이버 연대 훈련'을 한미동맹이 주도할 수 있음. 사이버 훈련이 포함된 한미 간 정례 연합훈련은 인태지역에서의 사이버전을 염두에 두어야 하고, 특히 그러한 훈련에 있어서 인태 지역의 사이버 안보를 위협하는 북한의 사이버 공격 대응에 있어서 한국의 주도적인 역할을 가정해야 함.
- 인태지역은 국가의 사이버 전력을 공격력에 중점을 두고 있는, 사이버 공격 역량이 세계 2위, 3위인 러시아, 중국뿐 아니라 가상자산 탈취에 있어 전 세계 최고 강자인 북한의 위협이 두드러지는 곳임.
- 전 세계 멀웨어 공격의 최대 근원지는 중국(2022년 전 세계 1위, 18.8% 차지)이고 이러한 멀웨어 공격의 최대 피해국은 미국이며, 최근 미국은 북한의 전체 사이버 공격의 42%를 받고 있고 한국은 15%로서 현재 북

한의 사이버 위협의 최대 목표 대상은 한국에서 미국이 되었음(Recorded Future 2023년 조사결과)

- 인태지역은 전 세계 최고의 사이버 역량 보유국인 미국, 호주, 한국이 위치한 곳이고 이 세 국가는 모두 전 세계 최대 사이버 위협국인 러시아, 중국, 북한이 위치한 곳으로서 결과적으로 인태지역에서의 민주주의 우호국 및 유사입장국의 사이버 안보 협력은 전 세계 사이버 공간의 평화에 대한 기여가 가장 효과적일 것임을 예측하게 함.

- 한미 간 사이버 안보 협력은 앞으로 현재 양국이 중점을 두고 있는 북한의 사이버 위협뿐 아니라 인태지역 전체의 사이버 안보에 기여하고 이 지역의 사이버 평화와 디지털 협력을 통해 이 지역의 번영에 있어서도 핵심 축이 되는 것을 목표로 삼아야 함.

- 따라서 한미의 사이버 안보 협력은 인태지역 개발도상국에 대한 사이버 안보 차원에서의 지원과 신흥기술 분야 및 사이버 기술 관련 교육·훈련 제공을 포함해야 하고 한미의 사이버 안보 협력이 이 지역의 번영에도 기여한다는 평판 형성에 기여할 것임.

한·미 민간섹터 협력 촉진

- 러시아-우크라이나 사이버전에서 우크라이나의 사이버 역량 강화 및 사이버 작전 수행에 기여하고 있는 미국의 IT 기업인 구글(Google), 마이크로소프트(Microsoft), 아마존(Amazo), 메타(Meta)과 스페이스

X(Space X)와 같은 기업과 한국의 IT 기업이 양국의 사이버 안보 관련 기업 간 공조와 협력이 활발해질 수 있도록 양국의 국가 차원에서의 사이버 안보 협력 시 주요 이해당사자로서 참여시킬 필요 있음.

○ 한국의 플랫폼 기업인 네이버(naver)와 다음(daum), 카카오(Kakao)가 구글이나 메타와 같이 사이버 공간의 사이버 영향공작이나 딥페이크 유포와 같은 다양한 악의적 디지털 정보에 대한 강력한 플랫폼 정책에 의거한 명확한 조치를 취할 수 있어야 함.

- 현재의 중국 발 사이버 영향공작(influence operations) 활동이 급증하고 있고, 국내 성착취 딥페이크 영상 문제가 심각한 상황에서도 만약 그러한 역할을 민간섹터가 수행할 역량과 의지가 결여되거나 부재할 경우, 정부의 대책과 대안은 무엇인지 심각하게 고민해야 할 시점임.

3. 한·미·일 및 한·일 사이버 안보 협력

한미일 및 한일 사이버 안보 협력의 단기·장기 비전과 목표 담은 공동 성명 발표

○ 한미일이 ▲인태지역과 세계안보에 있어서 사이버 안보 협력을 통해 어떤 역할과 기여를 할 수 있는지, ▲3국이 현재 사이버 영역과 관련하여 어떤 공통의 위협에 직면하고 있는지, ▲3국이 현재 보유한 사이버 역량 수준은 어떠하고 3국 공조를 통해 어떤 역량을 발휘할 수 있을 것인지, ▲3국이 어떤 역량을 발휘하며 현재까지 공조해왔는지, 그리고 ▲3국이 앞으로 어떤 사이버 안보 목적을 달성하려는지 3국의 비전과 협력 목적

을 담은 문건을 공동성명의 형태로 공표할 필요가 있음. 즉 이러한 공동의 목소리를 명문화하는 행위를 통해 3국 사이버 안보 협력을 대내외적으로 공고히 해야 함.

- 한·미·일 모두 북한의 멀웨어 공격과 가상화폐 탈취 및 중국을 비롯한 권위주의 레짐의 다양한 형태의 사이버 첩보활동, 허위조작정보의 공격을 포함한 인지전(cognitive warfare)·사이버 영향공작에 심각하게 노출되어 있음.
- 3국 중 일본의 사이버 능력이 제일 하위이나 그러한 일본의 약점이 한국과의 사이버 안보 협력을 통해 한국과 일본은 양국 간 신뢰와 연대를 강화할 수 있음.
- 2024년 라인야후 사태는 일본보다 우위에 있는 한국의 사이버 안보 능력에 대한 일본의 의구심을 불러일으킨 면이 있으므로 한국의 민간 섹터의 사이버 보안 문제는 한국의 사이버 역량 평판에 타격을 줄 수 있는 사안으로 인식해야 함.

○ 사이버 범죄 차단을 위한 한미일 혹은 한일 합동작전이나 사이버 군사훈련은 협력과 공조의 효과가 즉각적이고 가장 쉽게 빠른 연대 구축 효과를 노릴 수 있는 방법임. 미국을 중심으로 한 한미일의 사이버 안보 협력은 한국과 일본이 상대와의 협력을 '이익'으로 인식하는 데에 기여할 것이므로 미국과의 3자 협력을 강화하는 것은 일본과의 협력 환경을 양국에 우호적으로 조성하는 데에 기여할 것임.

○ 사이버 안보 협력은 가시적인 성과와 실질적 상호 이익이 가장 빨리 나타날 수 있는 영역이고 한국 국내 정치로부터도 비교적 자유로울 수 있

는 협력의 분야이므로 한국과 일본이 그 어떤 다른 군사안보 영역보다도 가장 적극적으로 추진해야 하는 분야임.

- 양국 협력에 동기부여를 최대화하기 위해서는 일본의 사이버 안보 능력의 약점과 취약점을 우리 편에서 파악하고 그러한 분야를 중심으로 협력을 제안하는 방법이 바람직함.
- 또한 우리보다 상대적으로 열악한 일본의 사이버 역량에도 불구하고 우리가 일본으로부터 얻을 수 있는 이익을 미리 식별하여 한국 대중에 대해 그 부분을 집중적으로 홍보하여 지지를 확보해야 함.

한미일 및 한일 정례 사이버 군사훈련과 국가 배후 허위조작정보 대응체제 추진

- 사이버 분야에서의 한미일 그리고 한일 간 상호신뢰와 연대감 구축의 효과를 위해 AI를 이용한 사이버 공격을 포함한 다양한 고도화된 외부 위협 시나리오에 대응하는 사이버 훈련을 정례화해야 함.
  - 사이버 안보 분야에서의 협력은 지상 혹은 해상에서의 군사훈련처럼 가시적인 군사력 동원 현장이 관찰되는 형태가 아니기 때문에 한일 간 다양한 갈등으로부터 비교적 자유로울 수 있음.
  - 한미일 혹은 한일 사이버 훈련 수행 시 적대국으로부터의 인터넷과 소셜미디어 공간에서의 대규모 허위조작정보의 유포 공격을 가장한 대응훈련도 포함할 필요 있음.

- 세 국가의 관계를 이간질하거나 분열시키려는 러시아, 중국, 북한으로부터의 시도가 지속되고 있으므로 한미일이 위협정보를 공유하고 한미일에 대한 국가 배후 허위조작정보 유포 활동에 대응할 버추어 플랫폼으로

서 한미일 '전략커뮤니케이션센터(strategic communication center)' 혹은 '정보상황실(information situation room)/정보퓨전센터(information fusion center)'를 구축할 수 있음.

- 이러한 플랫폼을 통해 3국이 사이버 안보 협력 비전과 목표, 일정이나 성과 및 향후 계획, 그리고 합동훈련 결과나 공동 연구결과 및 공동 행사 등을 대내외 청중과 미디어에 알릴 수 있으며 3국의 공통 인태전략을 홍보할 수 있음.
- 3국에 대한 사이버 위협이나 사이버 공간 상의 허위조작정보 적극적으로 동일한 메시지를 국제사회에 발신하고, 그러한 메시지가 3국의 인태전략과 어떻게 연결되는지 일관되게 전달해야 함.
- 이러한 3국의 플랫폼에 인태지역의 유사입장국이나 우호국들도 참여할 수 있게 하여 인태지역 사이버 안보 협력의 구심점으로 작동하게 해야 함.

4. 인태지역 소다자 그룹과의 사이버 안보 협력

Five Eyes, AUKUS, QUAD와의 사이버 안보 협력

- Five Eyes, AUKUS, QUAD 등은 이미 사이버 안보 부문에서 협력의 수준과 범위가 지속적으로 확장 및 강화되어 왔기 때문에 각 협의체의 소속 국가와 사이버 안보 협력을 도모하는 것은 각 협의체와의 협력 수준을 빠르게 증진시키는 효과를 가져올 것임.

- 이들 인태지역 소다자 협의체와 사이버, 해상, 우주 영역에서의 기술협

력과 방산협력 등 실질적 협력을 강화하여 상호간에 가시적인 이익을 발생시킬 필요가 있음.

- ▲사이버 위협정보를 공유하는 등 정보협력을 도모하고 ▲사이버 범죄 대응에 있어서 합동작전을 펼치거나 ▲사이버전과 각종 재난·재해 및 하이브리드 위협이 동시다발적으로 일어날 수 있는 상황을 가정한 ▲사이버 위기 대응 모의 훈련을 정례화하는 등 인태지역에서 발생할 수 있는 안보위협의 다양한 시나리오를 염두에 둔 사이버 안보 협력을 소다자 협의체를 통해 도모할 수 있음.

- 각각의 소다자 협력에서 한국이 기여할 기술적 분야와 우리의 역할을 공고화할 수 있는 정책 어젠더 발굴이 필요하고 그러한 어젠더 발굴에서 우리가 어떤 전략적 이익을 누릴 것인지 명확한 목표에 따른 접근법을 개발해야 함.

호주와의 사이버 안보 협력을 Five Eyes, AUKUS, QUAD와의 사이버 안보 협력과 연계

- 2024년 5월 2일 제6차 한-호주 외교·국방장관 회의에서 양국이 사이버 및 핵심기술 정책 대화, 그리고 인공지능(AI), 양자 및 통신 기술을 포함한 핵심 신흥기술의 표준설정과 상호운용성 증진 협력을 논의했음. 한-호주 간 이러한 협력이 AUKUS 및 QUAD와의 협력으로 이어지도록 오커스와 쿼드의 사이버 안보 주요 의제를 한-호주 사이버 안보 협력의 의제로 삼을 필요 있음.

- 이번 회의에서 양국은 인태지역에서 아세안(ASEAN) 및 태평양도서국포럼(PIF)과도 협력하기로 하였으므로 동아시아 국가들과의 사이버 안보 협력 의제를 호주와 공동으로 추진하는 것도 양국 간 사이버 안보 협력을 강화하는 데에 기여할 것으로 보임.

- 호주는 인태지역에서 동남아 국가들에 대한 사이버 안보 분야에서 ODA 협력을 함께 추진할 수 있는 파트너임. 주요 기관망과 공급망 등에 대한 멀웨어, 랜섬웨어 공격의 피해가 막심하고 동남아시아 포함 아프리카, 중남미 등의 피해는 국가의 전반적인 열악한 디지털 역량 때문인 경우가 많은데다가 한국과 호주는 동남아를 경유한 다양한 공격을 받고 있음.

- 우리 정부는 호주와 동남아시아를 비롯한 개발도상국의 디지털 역량을 강화하는 다양한 사업을 양국의 강점을 살려 분업하여 추진하고, 이들 국가의 미국과 중국과의 서로 다른 관계에 따라 차별적인 협력 사업을 전략적으로 추진할 필요가 있음.

- 동남아 포함 개발도상국과 사이버 기술 협력을 도모할 때 강화된 연대를 통해 상호 이익 창출이 클 것으로 판단될 경우 기술뿐 아니라 한국의 사이버 교리와 훈련 프로그램도 함께 진출시킬 필요가 있음.

5. 유럽 및 NATO와의 사이버 안보 협력

유럽의 하이브리드 위협 대응 위기관리 기관에 참여

○ 한국이 사이버 위협 등 다양한 하이브리드 위협에 대해 유럽과 동질적인 이해와 협력을 도모할 수 있는, 접근이 어렵지 않은 기관으로서 핀란드 헬싱키(Helsinki)에 위치한 '유럽 하이브리드 위협 대응센터(European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE)'와의 협력을 추진해볼 필요가 있음.

- EU는 2016년을 전후로 하이브리드 위협에 대응하기 위한 다양한 조직을 설치했고, 2017년 10월 EU이사회와 대서양위원회(North Atlantic Council)는 미국과 유럽 8개국 - 영국, 프랑스, 독일, 폴란드, 스웨덴, 핀란드, 라트비아, 리투아니아 – 이 중심이 되는 Hybrid COE를 설치함.
- Hybrid CoE는 하이브리드 위협 대응에 있어서 NATO와 EU간 전략적 토론과 훈련을 촉진하고 위협 대응의 모범사례를 개발하며 연구결과를 역내에 공유하는 기능을 담당.
- Hybrid COE가 주최하는 'Cyber Power Symposium on Hybrid Conflict and Warfare(CPH)'에 2023의 경우 일본, 호주, 우크라이나 등이 참여했고, 이 심포지엄에서는 사이버뿐 아니라 사이버 위협과 하이브리드 위협의 연결성, 사이버 방어 차원에서의 인지전과 하이브리드전의 관계성, AI 기술과의 관계 등을 논의함.

NATO 전략커뮤니케이션 센터에 참여

○ 유럽의 사이버전, 하이브리드전, 인지전에 대한 접근법은 NATO전략커뮤니케이션센터(NATO Strategic Communication Centre of Excellence, StratCom COE)에서 논의되고 형성된다고 해도 과언이 아닐 만큼 NATO StratCom COE는 유럽과의 사이버 안보 협력에 있어서 한국이 접촉하고 빈번하게 교류해야 할 기관임.

- 2014년 라트비아에 설립된 NATO StratCom COE는 NATO 회원국과 파트너 국가들의 전략커뮤니케이션 역량을 증진시키는 것을 목표로 다양한 연구, 분석, 개념 개발, 실험, 독트린 개발, 교육 및 훈련을 담당함.
- NATO StratCom COE는 현재 한국이 2022년 회원국으로 가입한 NATO Cooperative Cyber Defence Centre of Excellence(CCCDCOE)와 긴밀한 협력관계에 있으므로 한국의 접촉이 용이할 뿐 아니라 NATO StratCom COE에 현재 호주와 프랑스 등도 가입 과정을 추진하는 등 모든 NATO 국가가 회원국은 아님(현재까지 회원국은 라트비아, 에스토니아, 독일, 이탈리아, 리투아니아, 폴란드, 영국, 네덜란드, 핀란드, 스웨덴, 캐나다, 슬로바키아, 덴마크, 미국, 헝가리임).
- 한국의 정보기관, 군, 외교부 등 사이버 안보 분야에서 타국과의 전략커뮤니케이션을 담당할 기관이 NATO StratCom COE와 MOU를 맺고 민간섹터의 IT 기업, 연구소 및 학계 등이 함께 협력할 수 있도록 지원하는 역할을 맡을 필요가 있음.

사이버 공간에서의 허위정보/허위조작정보 공격 및 인지전 대응 협력

○ 한국은 지난 몇 년간 미국, 유럽, 호주 등의 국가로부터 국가 배후 허위조

작정보에 대한 대응과 인지전 관련 논의와 관련하여 협력의 파트너로서 인식되어 왔고 현재 정보기관, 외교부와 국방부는 이러한 이슈에 대한 대응 및 국제협력을 최근 시작했음.

- 특히 국정원 산하 국가사이버안보센터(NCSC) 합동분석협의체는 민간 보안회사들과 협업하여 중국의 사이버 영향공작 활동을 적발했고 이러한 상황을 구체적으로 다룬 보고서 "중국의 언론사 위장 웹사이트를 악용한 영향력 활동: 뉴스와이어 서비스 악용을 중심으로"를 2023년 발간한 데 이어 2024년 여름 영문의 번역 보고서 "China's Malign Activities by Exploiting Fake News Websites"도 발간함.

- NATO, EU는 사이버 기술뿐 아니라 인공지능 기술이 본격적으로 동원되는 허위정보/허위조작정보 유포 활동(mis/disinformation campaign) 및 인지전에 대한 기술적, 제도적, 위기대응체제 및 군사적 대응체제 갖춰오고 동유럽 지원 및 사이버 모의군사훈련 지속해왔으며, 이 분야에 대한 논의와 대응을 2016년부터 8년간 이어온 상태임. 그 결과 러우전쟁에서 NATO가 우크라이나의 사이버 심리전 혹은 인지전의 성공적인 수행에 지대하게 기여했고, 러시아의 심리전은 2014년 우크라이나 침공 시와 비교할 때 우크라이나 대중과 국제사회에 대한 프로파간다 영향력을 발휘하는 데에 실패함.

- NATO의 허위조작정보 대응 및 인지전 관련 연구는 NATO CCDCOE와 NATO StratCom COE을 중심으로 진행되고 있으므로 우리의 NATO의 인지전 대응 논의에의 참여 자체가 어려운 일이 아닐 뿐 아니라 NATO는 한국의 참여를 굉장히 환영할 가능성이 매우 높음.

- 현재 외교부의 외교전략정보본부는 FIMI(Foreign Information Manipulation & Interference)와 관련하여 인태지역 우호국들과의 협력을 논의하기 시작했음. FIMI는 단순히 여론전이나 커뮤니케이션 교란의 수준을 넘어서서 국가 위기 시에는 군사활동 즉 군사작전으로서 수행되고 있고 주로 사이버 공간을 전장으로 사용하고 있기 때문에 국가 안보 및 사이버 안보 차원에서 다루는 것이 적합함.

- 평시 중국이나 북한 등에 의한 영향력 공작은 국정원의 소관 사항일 수 있으나 평시와 전시의 경계에 제한받지 않고 수행되는 사이버전에는 늘 허위조작정보의 공격 등 인지전의 공격이 필수적으로 동반되므로 외교부와 군의 인지전 대응을 위한 대응체제 마련이나 법제도적 준비 등이 매우 시급한 상황임.

Naming & Shaming 지속

- 한국은 영국과 북한의 공급망 공격에 대한 합동주의보(2023.11.23.)를, 독일과는 북한의 사이버 첩보 활동에 대한 합동주의보(2024.2.23.)를 발표하는 등 유럽의 유사입장국과 규칙기반의 사이버 안보 질서를 추구하고 사이버 공간에서의 책임 있는 국가 행위를 강조하기 위한 공동의 목소리 내기 즉 'naming & shaming' 전개했음.

- 한국과 비슷한 수준의 사이버 역량을 가진 네덜란드는 한국과의 사이버 안보뿐 아니라 Reaim(Responsible AI in the Military Domain Summit) 공동 주최 등 인공지능 분야에서도 협력을 추구하고 타진해온 국가로서

유럽에서 한국의 주요 사이버 안보 협력 파트너로 자리매김하고 있으므로 유럽과의 협력에서 네덜란드와의 네트워크를 활용할 필요.

인태지역의 전략커뮤니케이션 센터 혹은 인태정보상황실 설립

- NATO의 전략커뮤니케이션센터 인태지역 지부 혹은 인태정보상황실(Indo-Pacific Information Situation Room)을 한국에 설치하여 인지전 공격 메시지 혹은 허위조작정보 확산 시 동맹·우호국·민주주의 유사입장국과 신속하게 정보와 분석을 공유하고 외교적, 기술적, 군사적 지원을 제공하며 공동의 정책결정을 추진하는 일련의 과정을 담당할 경우 우리의 전략커뮤니케이션 능력이 획기적으로 빠르게 증대할 수 있음.

- 이러한 센터나 상황실을 설치하고 운영하는 데에 있어서 정보기관, 외교부와 국방부가 함께 공조하면 위협정보에 대한 식별과 공유 및 분석 과정이 대단히 효율적으로 작동할 수 있음.

- 인지전 대응이나 허위조작정보에 대한 대응 노력이 현재 전 세계적인 추세이자 국제사회의 주요 현안임을 국내에 지속적으로 알리고, 한국의 인지전 대응도 국제사회에서의 공동의 노력에 부응하는 차원임을 지속적으로 알려야함. 이러한 메시지는 국내 정치적 변화 혹은 정권의 변화에 관계없이 인지전 대응이 지속되게 만드는 명분으로 작동할 것임.

6. 결론

○ 앞서 논의한 사이버 안보 협력을 위한 범부처 차원의 외교적 노력만큼 중요한 것은 우리 정부의 민간 섹터와의 협력이므로 국제무대에서 동등한 파트너이자 이해당사자로서 함께 진출하고 타국과의 협력 사업에 적극적으로 참여할 수 있도록 민간에 다양한 인센티브를 제공할 수 있어야 함.

- 정부와 민간의 공조가 오랜 기간 지속되면 민관의 유대 및 신뢰관계가 자연스럽게 강화되고 동일한 안보관과 위협인식이 형성되는 결과로 이어져 위기 시와 전시의 공조를 더욱 신속하고 효과적으로 만드는 결과를 가져올 것임.

○ 더욱 장기적으로는 국가 사이버 안보를 위한 다양한 공세적 활동의 일부를 민간이 위임받아 수행할 수 있도록 우리의 민간섹터의 사이버 안보 역량 강화를 적극 지원하고 보안 분야에서의 국내외 시장을 획기적으로 확장시켜야 함.

- 정부는 신뢰할 수 있는 민간 파트너(IT 회사, 플랫폼 회사, 사이버 보안 회사와 연구기관, 학계 및 민간의 전문가층, 언론 등)를 신속하게 식별하고 국가 간 협력과 프로젝트 착수 시 반드시 이들을 포함시켜야 함.

○ 불확실성이 강한 미래 군사안보 환경을 감안할 때 사이버 공간에서의 국가의 정보역량과 정확한 상황인식(situational awareness)이 더욱 중요해질 것이므로 사이버 공간에서의 위협을 더 잘 파악하고 예측해내는 데에 있어서 정부 각 부처의 상호 정보공유가 더욱 활성화되는 것을 넘어

상시 컨택이 가능한 24/7 체제를 갖추어야 함.

- 특히 사이버상에서의 위기에 대한 대응에 있어서 부처 간 일관되고 통일된 정책결정과 국내와 외부에 대한 일관된 메시지의 발신 즉 전략커뮤니케이션(strategic communication) 혹은 위기커뮤니케이션(risk communication) 차원에서의 긴밀한 공조체제 마련이 시급함.

제9장

사이버안보의 국제규범 외교 및 지역협력 외교

이 정 환 | 서울대학교 정치외교학부 교수

1. 사이버 안보 컨트롤타워의 효과적 가동
2. 사이버 안보의 범부처 공조 체계 정비
3. 사이버 안보 분야 민관협력 체계 정비
4. 사이버 안보 외교의 추진체계 정비
5. 사이버 안보 분야 법제도 정비

제9장

사이버안보의 국제규범 외교 및 지역협력 외교

이 정 환 | 서울대학교 정치외교학부 교수

배경과 구성

- 대한민국 정부의 <국가사이버안보전략>은 3대 목표 중 하나로 '글로벌 리더십 확장'을 추구하고 있으며, 이는 '사이버공간에서 자유, 인권, 법치의 가치를 수호하는' 규범적 성격을 지님.
- 사이버 안보 국가책략(cybersecurity statecraft)의 관점에서 보는 글로벌 리더십의 확장은 국제규범 외교와 지역협력 외교를 통해 달성될 수 있는 전략 목표임.
- 한미협력, 한미일협력, 한영협력, 인태지역 주요국과의 협력 등을 중심으로 하는 양자 협력 및 소다자 협력과 함께 유엔, 나토, G7 등의 글로벌 다자 공간에서의 규범 형성 과정에의 적극적 참여 사이의 균형 잡힌 외교 전략이 요구됨.
- 제9장은 한국이 국제규범 외교와 지역협력 외교를 바탕으로 사이버 안보 분야 글로벌 리더십을 확장해나갈 수 있는 구체적 방법을 모색함.

- 본 장의 구성은 아래와 같이 다섯 가지 항목을 중심으로 함.

  1. <국가사이버안보전략>과 국제규범 외교 및 지역협력 외교
  2. 사이버안보 분야 유엔외교
  3. 국제 사이버 규범 및 신뢰구축 형성 과정에의 참여
  4. 사이버안보 관련 가치외교
  5. 사이버안보 지역협력 구상 주도 및 글로벌 역량강화 지원 확대

1. 〈국가사이버안보전략〉과 국제규범 외교 및 지역협력 외교

○ <국가사이버안보전략> 3대 목표 중 두 번째 항목인 '글로벌 리더십 확장'

- 2024년 2월에 발간된 대한민국 정부의 <국가사이버안보전략>에서 '글로벌 리더십 확장'은 '공세적 사이버 방어 및 대응'과 '건실한 사이버 복원력 확보'와 함께 핵심 목표로 제시되고 있음.
- '글로벌 리더십 확장'은 한미동맹을 중심으로 하는 자유민주주의 국가와의 협력 뿐만 아니라, '사이버공간에서 자유, 인권, 법치의 가치를 수호하는' 규범적 성격을 지니고 있음.
- 사이버안보 분야의 외교는 '사이버공간에서의 책임있는 국가행동을 위한 관련 규범의 발전'을 지향하고 있으며, 이를 위한 국제공간에서의 규범 창출 능력이 요구됨.
- '각국의 수준과 목표에 부합하는 맞춤형 협력'은 한미협력이나 선진국가와의 공조 뿐 아니라, 사이버안보 분야 신흥국에 대한 적극적 지원의 협력 외교가 요구됨.

○ ‘글로벌 사이버 공조체계 구축’ 과제에서 국제규범 외교

- <국가사이버안보전략>의 다섯 전략과제 중에서 두 번째로 제시된 ‘글로벌 사이버 공조체계 구축’의 첫 번째 수단은 ‘미국을 비롯한 다양한 국가와의 사이버안보 협력 공고화’이고, 두 번째 수단은 ‘국제 사이버 규범 논의 및 신뢰구축조치 이행활동에 적극 참여’
- 한미협력, 한미일협력, 한영협력, 인태지역 주요국과의 협력 등을 중심으로 하는 양자 협력 및 소다자 협력과 함께 유엔, 나토, G7 등의 글로벌 다자 공간에서의 규범 형성 과정에의 적극적 참여 사이의 균형잡힌 외교 전략이 요구됨.
- ‘국제 사이버규범 논의 및 신뢰구축조치 이행 활동에 적극 참여’의 구체적 방법론으로는 다음과 같은 방법이 제시되고 있음.
  · UN、NATO 등의 사이버공간에 대한 국제법의 해석과 적용 등 국제사회 논의에 주도적으로 참여하여 규범에 기반한 사이버공간의 질서형성을 촉진
  · 기존 국제법과 규범의 이행에 관한 국제사회의 논의에 동참하고, 초국경 사이버 위협에 효과적으로 대응하기 위한 양、다자협력을 강화
  · 자국 정보통신시스템이 이용된 악의적 사이버 활동에 대한 영토국의 책임이 국제법적 의무라는 입장을 재확인하고 공감대를 구축
  · 악의적 사이버활동에 대한 국가안보적 위협 인식과 우리의 판단 및 대응에 관한 정책과 근거를 주기적으로 공개하여 우리 사이버안보 정책의 투명성과 신뢰를 제고
  · 기존의 정부 간 사이버안보 정책 협의를 우리의 국격과 위상에 걸맞게 다양한 국가로 확대하여 상호 간 이해와 신뢰를 증진함으로써 글로벌 사이버안보 위협을 억지하고 긴장 고조를 방지

· 新기술, 데이터 이전 등 다양한 사이버안보 관련 국제표준, 규범, 통상협정 등에 우리의 국익과 안보적 고려가 반영될 수 있도록 국제사회내 영향력을 강화

- 사이버공간의 자유, 인권, 법치의 가치를 글로벌 확산시키는 명확한 목표를 달성하기 위해 유엔, 나토 등의 국제무대에서의 사이버안보 규범 창출 논의에의 적극적 참여가 필요함.
- 다만, 사이버안보 규범 창출에 있어서의 주도성과 수용성의 균형감이 필요함. 주도성에 대한 과도한 의지보다는 주도성을 발휘하는 것이 가능한 부분과 수용적 자세 유지가 보다 효과적 부분에 대한 전략적 분리 대응 자세도 요구됨.

○ 사이버안보 지역협력 외교와 능력구축 지원 외교의 중요성

- <국가사이버안보전략>에서 강조하는 '각국의 수준과 목표에 부합하는 맞춤형 협력'은 한국에게 신흥국과의 협력에 대한 새로운 방법론 모색을 요구하고 있음.
- 한국의 사이버안보 외교의 중심축은 한미 간 「전략적 사이버안보 협력 프레임워크」를 중심으로 하는 한미동맹이지만, 사이버안보 분야의 능력이 부족한 신흥국에게 사이버안보 능력 지원 구축 외교를 통해, 한국의 국익과 위상을 제고할 수 있음.
- 사이버안보 분야 신흥국 중에서 인태지역 근린 국가들에 대한 적극적 협력 체계 구축을 통해서, 인태지역에서 한국의 국가 위상을 제고하는 효과적 방법론으로 사이버안보 지역협력 외교를 고려할 수 있음.

2. 사이버안보 분야 유엔외교

○ 사이버안보 분야 유엔외교 목표

- 사이버안보에 대한 글로벌 규범 형성 및 확산의 무대로서의 유엔공간에 대한 대응 전략 모색
- 미국 등 강대국의 사이버안보 규범, G7 사이버안보 규범 등과 함께, 경쟁적 사이버안보에 대한 논의의 무대로서의 유엔공간 대응 전략 모색

○ 사이버안보 규범 창출 무대로서의 유엔의 역할과 한계

- 사이버공간의 국제규범 형성 노력의 주요 무대로 유엔이 기능해 왔음.
- 유엔의 사이버안보 정부 전문가 그룹(GGE)회의: 2004년 이후 6차례 설치. 사이버안보에 대한 가장 중요한 국제사회 논의의 장
- 개방형워킹그룹(Open-Ended Working Group, OEWG)의 등장: 제6차 UNCGE와 병행
- GGE: 소수의 전문가로 구성 vs. OEWG: 모든 유엔 회원국에 개방
- GGE 합의 내용: 3차 회의에서 “기존 국제법과 주권의 온라인공간 적용” 원칙, 제4차 회의에서 주권 평등 및 내정불간섭 원칙 적용의 명확화
- GGE 5차에서 사이버공격에 대한 자위권 행사, 국제위법행위에 해당하는 사이버 조작에 대한 대응 조치, 사이버공간에 대한 국제인도법 적용 합의가 실패함.
- GGE 5차 이후 미국 등 선진국은 사이버안보 규범 창출 무대로 G7을 활용하고자 함.
- 미국의 유엔공간에서의 사이버안보 국제규범 형성에 대한 관심 저하,

양자 및 소다자를 중심으로 하는 진영적 사이버안보 외교를 지향

- 하지만, 사이버안보 국제규범 논의 공간으로서의 유엔 역할은 배제되기 어려움.

○ 유엔에서 기능적 어젠다 중심의 사이버안보 외교 필요성

- 한국: 2024-2025년 비상임이사국으로 한국의 핵심 관심 분야로 사이버 분야를 포함시킴. 이는 사이버문제가 글로벌 평화 문제와 직결된다는 한국의 의지를 반영하고 있음.
- 하지만, ACD 개념이 실제 보편화되는 추세와 별개로, 사이버안보에 대한 유엔공간에서의 국제법적 합의 형성은 쉽지 않은 상황
- 유엔공간에서는 국제법적 합의보다는 실제 사이버안보 침해 사례를 중심으로 하는 안보 문제를 환기할 필요성이 있음.
- 다만, 사이버안보 분야에서 한국이 가장 긴요하게 고민하고 있는 북한의 사이버침해 문제는 유엔 공간에서 적극적으로 제시하는 것에 있어서 한계가 있음.
- 북한의 사이버공간에서의 침해 문제는 한미협력과 한미일협력을 중심으로 대응하는 한편, 유엔 공간에서는 보다 일반론적인 침해 문제를 중심으로 논의를 전개할 필요가 있음.

3. 국제 사이버 규범 및 신뢰구축 형성 과정에의 참여

○ 국제 사이버 규범 및 신뢰구축 형성 과정에의 참여 목표

- 사이버공간에 대한 국제법의 해석과 적용 등 국제사회 논의에 주도적으로 참여하여 한국 국가 이익에 부합하는 사이버공간 규범 질서 형성 촉진 방안 검토
- 신기술, 데이터 이전 등 다양한 사이버안보 관련 국제표준, 규범, 통상 협정 등에 대한 대응 방안 검토
- 악의적 사이버활동에 대한 영토국의 책임의 국제법적 의무 해석의 확산 방안 검토
- 사이버공간에서의 책임 있는 국가 행동을 위한 관련 규범의 발전 방안 검토

○ G7의 사이버안보 국제규범 논의에의 적극 관여 필요성

- G7의 회원국은 아니지만, G7 확대회의 참여국으로 G7 회의에 지속해서 초청되고 있음.
- 일본에서 개최된 2016년 G7 정상회담에서 나온 「사이버에 관한 G7의 원칙과 행동」 문서: '사이버공간에서의 무력공격에 대해서 국가가... 국제연합헌장 제51조에 의거해 개별적 그리고 집단적 자위권의 고유의 권리를 행사한다고 인식'한다는 기술이 포함
- G7의 국제규범은 사이버공간에서의 침해 중 일부를 전통적 안보 차원의 무력 공격으로 위상 지우고 있으며, 이에 대한 국가로서의 대응 자세를 분명하게 하고 있음.

- G7의 사이버안보 규범 논의에 한국의 입장이 반영될 수 있는 적극성이 필요함.
- 사이버안보 외교 과제는 아니지만, G7이 글로벌 규범 창출과 확산의 중요한 수단이 되기 위해서는 G7의 확대가 필요하고, 이 확대에서 한국이 중심적으로 포함되어야 하는 상황임을 G7 국가들을 대상으로 적극 설득하여야 함.

○ 나토의 사이버안보 국제규범 논의에의 적극 관여 필요성
- 사이버안보 분야에서 나토는 유럽 지역을 넘어 전세계적 역할을 수행하고 있음.
- 한국은 2022년 나토의 사이버방위협력센터의 기여국으로 가입하고, 나토의 사이버방위협력센터가 주관하는 Locked Shields에 참여하고 있음.
- 나토 사이버방위협력센터는 나토 지역 이외의 민주주의 국가들을 대부분 포함하고 있어서 실제 사이버안보 분야의 자유 진영 협력 틀로 기능할 가능성이 큼.
- 더불어 나토의 CCDCOE(Cooperative Cyber Defense Centre of Excellece)는 사이버안보 규범 창출의 중심 무대로 기능하고 있음.
- CCDCOE의 탈린매뉴얼이 사이버안보 규범의 핵심 문서로 계속 발전하는 상황에서 나토 CCDCOE에 대한 한국의 적극적 관여가 요구됨.
- 다만 정부추천을 받지 않는 CCDCOE의 전문가 그룹에 정부 차원의 영향력 확보는 한계가 있음.
- 사이버안보 국제법 관련 한국인 국제적 전문가 육성을 통한 자연스러운 CCDCOE에 대한 장기적 대응 계획이 필요함.

4. 사이버안보 관련 가치외교

○ 사이버안보 관련 가치외교 목표

- 사이버안보 대응 체제 구축이 민주적 감시 및 통제의 원칙과 부합 발전할 수 있는 거버넌스 구축 방향 모색
- 디지털 사회의 기본 가치와 사이버안보에 대한 규범 형성 및 해외 확산 전략 모색

○ ITU에서 사이버공간의 민주주의 원칙 강조 필요성

- 사이버안보에 대한 규범이 한국이 지양하는 민주주의 원칙과 부합해서 발전하도록 하기 위한 외교는 양자, 소다자는 물론 유엔, 나토, G7 등의 무대에서 당연히 이루어져야 함.
- 더불어 각국 정부와 관련 민간 부분의 IT분야에 대한 국제적 논의 공간에서 자유, 인권, 법치에 입각한 사이버공간의 규범의 중요성과 이 규범에 부합하는 사이버 정책을 제기할 수 있어야 함.
- 유엔 전문기구로 국제전기통신 관련 문제를 다루는 International Telegraph Union은 사이버안보의 국제사회 논의 공간으로서 그 중요성이 큼.
- 2001년 정보사회세계정상회의 개최로 ITU는 사이버안보 논의의 중요 공간으로 위상 제고
- ITU는 사이버 분야를 포함한 정보기술 분야의 표준설정 무대
- 정보통신 분야의 표준설정 및 국제협력에서 자유, 인권, 법치 원칙의 준수에 대한 우호국들과의 공감대 형성 및 우호세력 확대 필요성

- 자유, 인권, 법치의 가치에 입각한 규범이 개도국들의 국가 이익과 부합함을 적극 발신할 필요성 (지역협력 및 ODA와 연결)

○ 민주주의 정상회의 및 인터넷 미래선언

- 2024년 3월에 한국에서 개최된 제3차 민주주의 정상회의는 한국의 가치외교에 대한 국제적 리더십에 있어서 중요한 전기가 되었음.
- '미래 세대를 위한 민주주의'의 주제 속에서 제3차 민주주의 정상회의는 신흥 디지털 기술의 투명성, 개방성, 책임성있는 활용을 통한 민주주의 가치 확산과 발전을 강조하였음.
- 제3차 민주주의 정상회의에서 강조된 기술의 책임성 있는 활용과 허위정보 대응 과제는 사이버안보와 직결되어 있는 것으로, 향후에도 한국의 사이버안보 국제 규범 형성 외교에서 민주주의 정상회의는 중요한 무대로 기능할 수 있으며 적극적으로 활용할 필요성이 있음.
- 한편 2022년 미국이 주도한 '인터넷 미래선언'에 한국이 파트너로 공식 참여함으로서, 한국의 사이버안보 가치외교에서의 적극성이 보다 강화되었음.
- '인터넷 미래선언'이 미국 주도로 발전하는 가운데, 이 선언의 내용이 한국의 국익과 가치에 부합하며, 포괄성있게 발전할 수 있도록 면밀한 대응이 요구됨.

5. 사이버안보 지역협력 구상 주도 및 글로벌 역량강화 지원 확대

○ 사이버안보 지역협력 구상 주도 목표

- 아시아태평양, 동아시아 지역에서의 다양한 다자협의체에서 사이버안보 어젠다 형성 전략 모색 (사이버 동평구)
- 사이버안보 한미일 협력, 나토 및 G7 협력과 더불어 사이버안보 전략의 글로벌 공간 지평 확대 및 전방위적 성격 확보를 위한 지역협력 모색
- 한중일 삼국협력에서 사이버안보 협력을 어젠다화할 수 있는 방안 모색

○ 한미협력과 공진화하는 지역협력

- 미중경쟁 시대 인도태평양 지역 내 구도가 진영화하는 가운데, 한국 외교의 다면성이 감소할 수 있다는 우려도 존재
- 미중경쟁 시대 강대국에 대해 헷징하기 위한 중견국, 개도국의 고민 속에서 지역협력의 가능성이 장기적으로 새로 주목받을 가능성이 큼.
- 미국 주도의 소다자 협력에 적극적으로 임하는 가운데, 다른 한편으로 아시아의 중견국, 개도국과의 기능적 협력을 지속해서 발전시킬 필요성이 있음.
- 기능적 지역협력 발전의 중요 방법으로 사이버안보 분야는 한국의 외교 역량이 큰 분야이기도 함.
- 동아시아 지역에서 중견국과 개도국이 (미국과 중국을 제외하고) 가장 신뢰할 수 있는 사이버안보 협력 파트너로 한국이 고려될 가능성이 큼.
- 인도태평양 지역 공간에서 한국의 자체적 위상 제고를 위한 방법으로

사이버안보 역량을 외교적으로 활용할 수 있음.

- 핵심적으로 동남아지역 국가들과의 사이버안보 협력 제고가 모색될 수 있음.
- 매년 가을에 이루어지는 아세안 관련 정상회담에서 사이버안보 분야 논의를 주도할 필요성이 있음.
- 아세안과의 협력은 아세안+3, 한중일 협력과도 연결됨.
- 북한의 사이버 공격 특정을 위한 중국과의 협력도 현실적으로 필요한 가운데, 동아시아 지역협력 틀을 통한 중국과의 협력 논의 공간을 확대 창출할 필요성이 있음.

○ 사이버안보 ODA를 통한 글로벌 역량강화 지원 확대 목표

- 세계 각국이 사이버 위협에 대응하고 안전한 사이버공간 구축에 참여할 수 있는 역량강화 지원사업 전략 모색
- 기술적, 물적 자원 중심의 지원에서 국가 전략, 법제, 정책 수립 역량까지의 종합적 지원전략 모색
- 안보협력 차원의 능력지원 구축사업과의 연계 및 보안기술협력 차원의 협력 강화를 종합적으로 모색할 방안 탐구

○ 사이버안보 ODA에 대한 증가하는 관심

- 사이버안보 전략 및 정책 수립, 법제도 형성, 및 기술 도입 및 인력 양성에 대한 국제적 도움을 기대하고 필요로 하는 개도국이 다수 존재
- 이들의 사이버안보 정책 추진에 대한 외부적 지원처로서 가장 선호되는 대상으로서 한국의 위상이 큼.
- 사이버안보 영역에서 한국의 국제적 위상이 높은 가운데, 미중 경쟁 시

대 한국의 중견국적 성격에서 기인하는 한국의 매력

- 글로벌 사우스 대응이 한국 외교의 시대적 과제로 부상하는 가운데, 한국의 장점을 살리는 외교 전략으로 사이버안보 ODA를 적극 활용할 필요성이 큼.

제10장

사이버 안보/ 외교와 민관협력

차 정 미 | 국회미래연구원 국제전략연구센터장

1. 사이버안보와 사이버 안보외교의 민관협력 과제
2. 사이버 안보의 진화와 AI-사이버 안보 민관협력 과제
3. 대국민 사이버 안보 인식 제고 및 민관협력 과제
4. 사이버 안보 국제컨퍼런스 개최 등 글로벌 리더십 강화 및 공공외교 추진 과제
5. 글로벌 거버넌스 대응 차원의 민관협력 과제

제10장

사이버 안보/ 외교와 민관협력

차 정 미 | 국회미래연구원 국제전략연구센터장

배경과 구성

- 2024년 2월 발표된 대통령실 국가사이버안보전략 보고서는 글로벌 차원의 공조, 신기술 경쟁우위, 국가 사이버 위협대응, 전문인력 양성, 대국민인식 제고 등에서 민관 협업의 중요성을 강조함
- 사이버 안보가 글로벌 외교협력, 군사안보협력, 산업경쟁과 기술경쟁의 핵심 요소로 부상하는 가운데 세계 주요국의 트렌드 또한 사이버 안보와 사이버 안보 외교, 민관협력을 밀접히 연계하는 방향으로 나아가고 있음
- 다만 민관협력이 정확히 무엇이며 또 어떠한 층위와 범위에서 이루어지는 협력을 의미하는가는 여전히 모호함. 따라서 정부와 민간 행위자 간 정보공유의 이점을 넘어 실질적으로 어떠한 분야에서 어떻게 협력해야 하는지에 대한 종합적 검토가 요구됨
- 이러한 맥락에서 한국은 글로벌 외교협력과 리더십 제고를 위한 사이버 안보 민관협력의 한국식 모델을 모색해 나갈 필요가 있음

- 제10장의 구성은 아래와 같이 다섯 가지 항목을 중심으로 함

  1. 사이버안보와 사이버 안보외교의 민관협력 과제
  2. 사이버 안보의 진화와 AI-사이버 안보 민관협력 과제
  3. 대국민 사이버 안보 인식 제고 및 민관협력 과제
  4. 사이버 안보 국제컨퍼런스 개최 등 글로벌 리더십 강화 및 공공외교 추진 과제
  5. 글로벌 거버넌스 대응 차원의 민관협력 과제

○ 본격적인 논의에 앞서 한국의 사이버 안보와 사이버 안보 외교의 민관협력 현황을 살펴볼 필요가 있음

○ 첫째, 민관협력, 글로벌 협력은 한국의 국가사이버안보전략 이행을 위한 중요한 축으로 강조

- 2024년 2월 발표된 대통령실 국가사이버안보전략 보고서는 △글로벌 사이버 공조체계 구축을 위한 민간 및 국제기구들과의 협력, △신기술 경쟁우위 확보 위한 민관 협력, △ 국가 사이버 위협대응, 전문인력 양성 및 훈련 △대국민인식 제고 및 실천강화 등에서 민관 협업 강조[1)]

1) 대한민국 대통령실 국가안보실, “국가사이버안보전략.” 2024.02.

【국가사이버안보전략(2024.02) 사이버 안보 외교 관련 세부 내용】

- 정부, 국내외 민간기업, 국제기구 등과 교류 확대, 민간 상호간 국제협력 장려·지원
- 1.5트랙 정책협의 등 국내외 정부 및 민간 전문가 논의의 장 추진
- 다양한 이해관계자들이 참여하는 사이버 안보정책 수립
- 개발도상국을 대상으로 한 역량강화 지원사업 추진
- 국가전략, 법제, 정책의 수립 역량까지 지원범위 확장
- 국제기구 및 주요 공여국과의 역량 강화 지원사업 조율

○ 둘째, 세계 주요국의 트렌드 또한 사이버 안보와 사이버 안보 외교, 민관협력 밀접히 연계

- 세계 주요국들은 사이버 안보 위협 공유, 공동대응, 인재양성, 글로벌 거버넌스, 사이버 안보외교, 사이버 안보 산업망, 기술 개발 등에서 민관협력의 중요성을 강조하고 협력의 제도화를 위한 체계 강화 추세 세계 주요국들은 사이버 안보 역량 강화와 글로벌 위상 제고를 위해 외교부, 정보부 등에서 사이버 안보 민관협력 전략과 정책을 구체화하고 있음. '광범위한 부문간 협력(Cross-sector collaboration)'이 사이버 위협 대응에 게임체인저라는 점에서 공공부문과 민간부문의 협력(PPP)이 세계적으로 주목받고 있음[2)]
- 가장 대표적인 사례가 미국 사이버 보안 및 인프라 보안국(CISA)의 JC-

2) Gary Steele, "Data and public-private partnerships are the future of cybersecurity," World Economic Forum, 2023.01.16
https://www.weforum.org/agenda/2023/01/data-and-public-private-partnerships-cybersecurity/

DC(Joint Cyber Defense Collaborative)로, 공공 및 민간 부문이 사이버 위험 정보를 적극적으로 수집, 분석 및 공유한다는 공통 목표를 가지고 협력하는 공동체[3)]

- 중국은 중국공산당 중앙군민융합발전위원회 산하에 치후360(360公司) 등 민간 사이버안보기업이 주도하는 '사이버안보 군민융합혁신센터(网络空间安全军民融合创新中心)' 설립, '미래 사이버전쟁에서의 승리'를 위한 민간부문의 협력 참여 촉진[4)]
- EU의회는 2016년 'Cybersecurity Public-private partnerships'을 출범시켜 EU위원회와 의회 차원에서 민관협력 지원.[5)]

○ 셋째, 지정학 위기와 사이버 안보 외교 민관협력 연구의 필요성

- 민관협력(Public-private partnerships, PPPs)은 사이버 안보전략의 중요 요소이나 정확히 무엇인지는 모호한 제안에 그쳐 왔음. 단순히 정보공유의 이점을 넘어 실질적으로 어떠한 분야에서 어떻게 협력해야 하는지

3) Gary Steele, "Data and public-private partnerships are the future of cybersecurity," World Economic Forum, 2023.01.16
https://www.weforum.org/agenda/2023/01/data-and-public-private-partnerships-cybersecurity/

4) 차정미 (2019), "미중 사이버 군사력 경쟁과 북한 사이버 위협의 부상," 『통일연구』 23 (1), p.64.

5) European Parliament, "Public-private partnerships for cybersecurity: In "Connected digital single market" 2024.05.20.
https://www.europarl.europa.eu/legislative-train/package-better-business-environment-for-digital-networks-services/file-public-private-partnerships-for-cybersecurity

에 대한 종합적 검토와 구체적 접근 필요[6)]

- 국가안보와 경제발전 차원에서 모두 사이버 안보의 중요성이 높아짐에 따라 주요국들은 민간기업과 정부간의 사이버 안보 관련 논의를 확대하고 협력 방안의 구체화 제도화를 강화해 가고 있음
- 2022년 미국 CSIS에서는 주요 기업의 정보보안 고위간부와 정부고위 관료들이 함께 공통과제를 식별하고 모범사례, 협력방안을 논의하는 비공개 원탁회의 개최[7)]
- 최근 우크라이나 전쟁과 이스라엘-하마스 분쟁 등은 사이버 안보 분야의 민관협력 필요성과 실질적인 실천방안의 구체화 요구
  · 특히 미중 경쟁의 지속과 심화 속에서 사이버 안보 분야가 유사입장국 안보 협력의 핵심 어젠다로 자리잡고 있다는 점에서 사이버 안보 외교력 강화를 위한 민관협력 부상(산업기술기업의 글로벌 협력 메커니즘)
- 우크라이나 전쟁은 사이버 안보를 위한 빅테크 기업과 정부간 협력의 중요성을 보여준 대표적 사례로, 사이버 안보전략과 정책, 전장에서의 정부-민간기업 협력체계 강화 요구

6) Jamie Collier, "Optimising Cyber Security Public-Private Partnerships," RUSI, 2021.05.28 https://rusi.org/explore-our-research/publications/commentary/optimising-cyber-security-public-private-partnerships

7) Eugenia Lostri, James Andrew Lewis, and Georgia Wood, "A Shared Responsibility: Public-Private Cooperation for Cybersecurity," 2022.03. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220322_Lostri_Public_Priatev_Cooperation.pdf?VersionId=aoeH8eOs0uhaBPp8HPVgi.qkEXFmj2yX

1. 사이버안보와 사이버 안보외교의 민관협력 과제

○ 첫째, 사이버 안보 민관협력과 관련하여, 안보는 국가의 책임으로 인식되나 사이버 안보의 대상인 인프라 대부분이 민간이 소유와 운영을 하고 있는 환경 속에서 국가와 기업, 민간사회의 연계가 존재[8)]

- 민관협력(Public-Private Partnership)은 정보를 공유하고, 위험을 공유.완화하는 메커니즘 역할을 하여, 사이버 안보에 필수적 요소[9)]
- 중국 시진핑은 "사이버 안보를 유지하는 것은 사회 전체의 공동책임"이라고 규정하고 "정부, 기업, 사회단체, 대다수 네티즌들의 참여가 필요하다"고 강조[10)]

○ 둘째, 사이버 안보와 민관협력의 중요성과 협력 분야의 지속 확장과 관련하여, 사이버 안보 민관 협력은 아래 그림과 같이 사이버 위협 대응과 기술혁신, 인재육성 등 국내적 사이버 안보 대응과 글로벌 안보협력, 기술협력, 규범협력, 개발도상국 지원 등 사이버 안보 외교 분야로 구분할 수 있음

8) Madeline Carr., "Public-private partnerships in national cyber-security strategies," International Affairs 92: 1 (2016) 43, p.54.

9) Carnegie Melon University, "Public-Private Partnerships: Essential for National Cyber Security," CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS, 2024. https://insights.sei.cmu.edu/documents/4517/2010_016_102_67854.pdf

10) 光明网, "学习语丨维护网络安全是全社会共同责任," 2023.09.14. https://baijiahao.baidu.com/s?id=1776981663786590490&wfr=spider&for=pc

〈그림 10-1〉 사이버 안보와 사이버 안보외교 민관협력(PPP, Public-Private Partnership)[11]

○ 사이버 안보 위협 정보 공유와 대응, 회복력 지원, 인재육성 등은 기존 연구와 논의에서도 민관협력의 핵심분야로 주목받아왔으나, 국제질서 변화와 진화하는 위협 속에서 사이버 안보 민관협력의 공간 지속 확대

- 글로벌 사이버 안보협력 부상, 사이버 안보 기술과 산업 경쟁, 글로벌 사이버 안보 공급망 재편 등의 이슈화 속에서 사이버 안보 PPP는 단순히 위협 공동대응 차원을 넘어 사이버 안보기술 혁신, 사이버 안보 경제 창출, 사이버 안보 인재 육성이라는 '발전'의 목표와 글로벌 사이버 안보 영향력과 위상 제고라는 '외교'의 목표 달성을 위해서도 핵심적 요소
- 사이버 안보 민관협력은 사이버 안보 위협대응, 기술과 산업발전, 글로

11) Petar Radanliev, "Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing," Journal of Cyber Security Technology, (Feb. 2024), p. 25.의 그림일부를 차용하여 저자가 작성

벌 시장 창출, 글로벌 협력, 글로벌 영향력과 위상 제고, 인재 교육 등 '안보-외교-발전'의 차원에서 전개

※ EU의회와 EU위원회는 2016년 사이버 안보 기술과 솔루션을 위해 '사이버 안보 Public-private partnership'을 출범시키고, 유럽의 사이버 회복력 시스템 강화와 경쟁력있고 효과적인 사이버 안보산업 육성에 대한 커뮤니케이션을 발표. EU위원회의 연구혁신 프로그램인 Horizon 2020에서 4억5천만 유로 사이버안보 PPP 예산 책정.[12)]

○ 셋째, 사이버 안보 역량강화와 민관협력 거버넌스 제도화와 관련하여, 사이버 안보 PPP 전략은 포괄적 개념(umbrella term)으로, 아래와 같이 보호, 위협대응, 시장경쟁력, 회복력, 국제협력 등 다양한 측면에서 강조

- 2023년 3월 발표된 미국 백악관의 'National Cybersecurity Strategy'는 5대 협력과제로 (1) 핵심인프라 보호 (2) 위협행위자 저지 및 해체 (3) 안보화 회복력을 위한 시장경쟁력 형성 (4) 회복력 기반의 미래 투자 (5) 공동의 목표 추구 위한 국제협력 촉진을 제시하면서, 다양한 측면에서 'public-private collaboration' 강조.[13)]

12) European Parliament, "Public-private partnerships for cybersecurity: In "Connected digital single market" 2024.05.20.
https://www.europarl.europa.eu/legislative-train/package-better-business-environment-for-digital-networks-services/file-public-private-partnerships-for-cybersecurity

13) The White House, "National Cybersecurity Strategy," 2023.03. p.32.
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

○ 특히 사이버 안보 위협공유와 공동 억지, 공동대응이 중요 과제

- 사이버 안보는 기밀주의와 비공개 회의 등 전통적인 정보 문화를 대외적 대응에 결합해야 할 필요성을 고려할 때 더욱 중요. 또한 민간조직들이 정부기관과의 제도적 연결을 구축하여 신뢰를 확보[14)]
- 미국 사이버보안 및 인프라보안국(CISA)의 JCDC(Joint Cyber Defense Collaborative)와 영국 국가사이버안보센터(National Cyber Security Centre, NCSC)가 공공부문과 민간부문 인재들을 함께 모아 위협대응에 협력하는 'Industry 100 Initiative'가 대표적 사례
- 영국 NCSC는 'Industry 100'을 보완하는 또 다른 민관협력 프로그램으로 Cyber League를 두고 있음. Cyber League 회원은 NCSC와 협력하여 위협 상황에 대한 고유지식과 이해를 제공하는 다양한 업계 전문가 그룹. 분석 워크숍과 토론 그룹 등 다양한 활동참여[15)]
- 미 국토안보부(DHS)의 "The Public-Private Analytic Exchange Program (AEP)" : 본 프로그램은 국가정보국(Office of the Director of National Intelligence, ODNI)의 재정지원으로 국토안보부가 수행하는 민관협력 촉진 프로그램. 국토안보부의 Office of Intelligence and Analysis(I&A), Engagement, Liaison, and Outreach Division, Private Sector Engagement Branch 등이 참여. 2024 AEP에는 60개의 정부와 64개의

14) Jamie Collier, "Optimising Cyber Security Public-Private Partnerships," RUSI, 2021.05.28 https://rusi.org/explore-our-research/publications/commentary/optimising-cyber-security-public-private-partnerships

15) UK NCSC, Cyber League: A community committed to cyber security. https://www.ncsc.gov.uk/information/cyber-league

민간 부문 참가. 정부 참가자는 연방 수사국, 군, 교통부, 국가안보국, ODNI, 주 및 지방 정부, 융합 센터를 포함한 17개 조직이며, 민간 부문 참가자는 Amazon, Secure Community Network, Meta, The Walt Disney Company 및 Cit 등임.[16)]

- 2024년도 AEP 주제에는 사이버안보의제 다수. 5G Impacts on Smart Cars and Highway Infrastructure Modernization, Impact of Artificial Intelligence on Criminal and Illicit Activities, 5G Impacts on Cybersecurity-Security Implications of 5G Technology, U.S. Maritime Trade and Port Cybersecurity 등임
- 사이버 안보 분야에서 민간기업과의 연계를 강화하기 위한 부처차원의 다양한 연구와 보고서 발표. 미 국방대학교의 "The New "Cyber" Space Race Integrating the Private Sector Into U.S. Cyber Strategy" 등[17)]

○ 한국도 영국의 'Industry 100 이니셔티브'와 미 국토안보부의 AEP와 같이 다양한 부처와 광범위한 민간기업와 전문가들이 함께 참여하는 연간 프로젝트 등을 통해 위협 공유와 위협대응을 위한 인프라 확산, 기술역량 제고, 사이버안보 프로그램 등 다양한 측면에서 협력 제도화 필요

16) "2024 Public-Private Analytic Exchange Program Kick-Off Release," 2024.03.05 https://www.dhs.gov/news/2024/03/05/2024-public-private-analytic-exchange-program-kick

17) https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-109/jfq-109_25-32_Alen-Eaton-Stieler.pdf?ver=gCDB8jzOyTQCm34cLAnedA%3d%3d

○ 넷째, 글로벌 사이버 안보외교, 기술외교 강화와 민관협력과 관련하여, 세계 주요국들은 글로벌 사이버 안보 협력 측면에서 사이버 안보 외교 강화

- 2016년에 설립된 호주의 사이버 역량 구축 프로그램인 사이버 및 핵심 기술 협력 프로그램(CCTCP)은 인도 태평양 전역에서 사이버 회복력 개선 추진. 2021년 발표된 International Cyber and Critical Technology Engagement Strategy에서도 민간부문과의 협력 강조
- 최근 주요국의 기술대사직(Tech Ambassador) 신설, 글로벌 빅테크기업에 대한 reach out과 사이버안보 협력 주력하는 기술외교 확대. 덴마크 등 기술대사들의 임무 중 사이버 안보 협력이 최우선 과제 중 하나로 명시[18)]
- 대만 디지털부장관은 2023년 영국의 OneWeb을 방문하여 비상위성통신 네트워크 구축 등 대만방위역량 강화를 위한 기술동맹 구축. 이후 OneWeb과 대만 인터넷업체 협력

○ 사이버 안보 전략 대화의 '외교-안보-발전' 복합구조

- 국가간 사이버 안보 협력을 위한 사이버 안보 대화가 위협대응은 물론, 기술과 산업, 글로벌 거버넌스 협력
- 2024년 5월 미국과 스웨덴의 사이버 디지털 대화(Cyber and Digital Dialogue)는 6G를 포함한 차세대 네트워크와 인공지능, 양자정보과학, STEM교육 등 연구 분야 협력 촉진 위해 미국국립과학재단, 스웨덴 혁

18) Office of Denmark's Tech Ambassador, "The TechPlomacy Approach," https://techamb.um.dk/the-techplomacy-approach

신청 비노바(Vinnova), 스웨덴 연구위원회 간 과학기술 연구 협력에 관한 양해각서(MOU) 체결[19)]

- 2023년 중러 사이버 안보협력협정 체결 시 양국 사이버 안보 기업은 기술연구개발과 시장협력 약속하는 MOU체결

○ 사이버 안보 기술외교의 중요한 축으로 사이버 안보 인재 육성 및 사이버 안보 교육

- 화웨이. 메이야피코(美亚柏科), 관안정보(观安信息) 등 중국 네트워크 기업들이 일대일로 국가들에게 사이버보안 분야 교육과 전문훈련서비스를 제공하는 사례 참고

○ 한국 또한 글로벌 사이버 안보외교 차원의 민관협력 강화 필요

- 한국의 사이버 안보 민관협력이 현재까지 대체로 위협공유와 위협 대응차원에 중점을 두고 있으나, 기술대사의 사례와 같이 해외 민간 기업과의 소통과 협력 등을 추진하는 '국내정부와 해외민간' '국내민간과 해외정부' 등 다양한 차원에서 사이버안보 민관협력 활성화할 수 있는 방안들 모색 필요
- 글로벌 사이버 안보 산업, 기술 협력 차원에서도 정부간 사이버 안보 외교의 틀을 적극 활용하면서, 인재교류와 기술산업협력을 확대해가

19) U.S. Department of State, "Joint Statement on the Inaugural U.S.-Sweden Cyber and Digital Dialogue," 2024.05.03.
https://www.state.gov/joint-statement-on-the-inaugural-u-s-sweden-cyber-and-digital-dialogue/

는 민관협력의 사이버 안보외교 필요

○ 한국은 전 세계에서 사이버 공격을 가장 많이 받는 국가 중 하나라는 점에서[20] 국가안보 차원에서는 물론 글로벌 사이버 안보 협력 공간에서 한국의 위상과 영향력 제고 차원의 민관협력 확대 강화 필요

- 사이버 공격 피해자의 상당수가 민간, 민간기업(특히 중소기업)들이라는 점에서 민간의 사이버 안보역량 강화를 위한 지원과 인센티브 제도화 필요. "시장이 안보강화의 동력을 가질 수 있도록" 정부는 민간이 사이버 안보의 중요성을 인식하고 적극적으로 사이버 안보 생태계 구축에 참여할 수 있도록 유인하는 다양한 조치들이 필요
- 또한 사이버 안보가 글로벌 외교협력, 군사안보협력, 산업경쟁과 기술경쟁의 핵심 요소로 부상하고 있는 환경 속에서, 한국은 사이버 위협 대응과 역량강화, 회복력 강화를 위한 민관협력은 물론 글로벌 외교협력과 리더십 제고를 위해서도 사이버 안보 민관협력의 한국모델, 한국방안을 모색할 필요
- 2023년 국정원 산하에 민관 공동대응 위한 '국가사이버안보협력센터'가 개소하고, 사이버 안보 인재 10만양성 등 민관 사이버 합동대응 역량 강화를 추진하고 있으나 여전히 사이버 안보 역량강화를 위한 민간 인식과 참여를 제고하는 생태계 구축과 민관협력을 통해 글로벌 사이버 안보 분야를 주도하는 노력들이 다양하게 전개될 필요

20) 2023년 10월 Microsoft Digital Defense Report에 따르면 한국은 우크라이나, 이스라엘 다음으로 가장 많은 사이버 공격을 받는 나라임 (4위는 타이완). Microsoft Threat Intelligence, 『Microsoft Digital Defense Report; Building and improving cyber resilience』 2023.10.

2. 사이버 안보의 진화와 AI-사이버 안보 민관협력 과제

○ 첫째, AI 사이버 안보와 민관협력 관련, 인공지능, 특히 생성형 인공지능은 정치 어젠다, 기업이사회 등에서 사이버 안보를 최상위 과제로 만들고 있음

- 2023년 9월 영국 National Cyber Secrity Center(NCSC)는 AI 기반의 안보 위협에 대응하고 안보를 확보하는 문제에 대해 기업에 대한 제언을 담은 보고서를 출판하였음[21)]
- 생성 AI 규범 등 신흥 사이버 안보이슈 관련 민관협력 거버넌스를 토대로 한국의 AI안전 전략 도출. 국내 민간기업과 정부, 학계가 참여하는 위원회 등 구성. 향후 출범하게 될 국가사이버안보위원회 산하 소위원회로 AI 사이버안보위원회 등 설립 검토

○ 둘째, 허위정보와 사이버 공간 안보, 민관협력 관련, 기술의 발달과 함께 허위정보, 해외 영향력 개입 등이 민주주의 국가들에게 중요한 관심어젠다로 부상. 글로벌 차원의 국제협력과 민관 협력 긴요

- 대만은 허위정보, 정보조작 등에 기반한 사이버 악성활동 분석과 대응에 사회전체적 접근방식 강조. 민관협력의 허위정보 대응 생태계 구축
- 외국 허위정보가 감지되면 담당부서가 검증완료하여 행정원 웹사이트

21) Owen Hughes, “Cyber League: UK’s NCSC Calls on Industry Experts to Join its Fight Against Cyber Threats,” January 24, 2024
https://www.techrepublic.com/article/ncsc-cyber-league/

에 게시하고, 기술역량과 글로벌 네트워크를 갖춘 수많은 fact-check 비영리 단체들이 활동. 시민사회의 대국민 미디어 리터러시 증진이 대만 사회의 허위정보 저항에 크게 기여

- 대만의 허위정보 대응 비영리 단체들은 해외 씽크탱크 및 전문가들과의 적극적 교류를 통해, 대만의 사례를 홍보하고 허위정보 대응의 주요 모델로 글로벌 사회의 강력한 네트워크 구축

○ AI기술의 발달과 최근 허위정보 대응에 대한 글로벌 협력의 확대 추세 속에서 한국 또한 새롭게 진화하는 사이버 안보 분야 민관협력 모델 구축 검토

3. 대국민 사이버 안보 인식 제고 및 민관협력 과제

○ 첫째, 대국민 사이버 안보 인식 제고 위한 강화를 위한 이른바 "whole-of-society approach"와 관련하여, 사이버 안보는 전국민, 전사회의 관심과 인식제고, 공동대응의 문화와 생태계가 가장 중요. 포괄적 사회참여가 미래 사이버 안보 역량강화와 회복력 제고에 핵심요소

- "전사회적 접근(whole-of-society approach)"을 강조하는 대만의 사이버안보 전략은 한국의 사이버 안보전략과 민관협력의 주요한 참고가 될 수 있음. 대만의 사이버 안보에 대한 전사회적 접근은 정부, 민간, 학계, 시민사회, 개인을 포함한 사회시스템 전체의 체계구축을 추구. 이 방식의 주요 특징은 통합, 협업, 포괄적 참여, 지식공동창출 강조

- 세계주요국들은 전사회적 접근을 위한 국민인식 제고 프로그램 다양하게 추진
  - 미 사이버 안보 인프라안보국(Cybersecurity and infrastructure Security Agency, CISA)은 사이버 안보 인식 제고 프로그램(Cybersecurity Awareness Program) 운영[22)]
  - EU사이버안보국(European Union Agency for Cybersecurity)은 "Awareness Raising in a Box (AR-in-a-BOX)" 패키지를 고안하여 민간과 공공부문의 사이버 안보 인식 제고 지원. 고객맞춤형 인식제고 프로그램, 퀴즈와 게임 등 사이버 안보 인식제고 패키지

- 한국의 사이버 안보전략 또한 '전사회적 접근'의 중요성을 견지하면서, 국민 개개인과 사회전체의 사이버 위협에 대한 관심과 인식제고 프로그램 활성화 필요

- 둘째, 사이버 위협 정보공개 및 공유 등 민간의 대국민 사이버 안보 인식 제고, 국익 위한 글로벌 위협 평가 역할

- 주요국의 기업들은 사이버 해킹 연례보고서, 사이버 위협평가 보고서 등을 통해 글로벌 사이버 위협의 지형과 환경에 대한 정보 공유 및 인식 제고에 역할

22) CISA Cybersecurity Awareness Program.
https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program

- 사이버 안보 위협평가 및 대응에 있어 민간기업의 리포트와 분석들이 정부 사이버 안보전략과 정책의 중요성, 타당성 등을 뒷받침하고, 국민들의 인식 제고에 역할
- 마이크로소프트는 4년 전부터 매해 『Microsoft Digital Defense Report』를 발행하여 사이버 위협의 진화를 분석하고 전략방향을 제시하고 있음. 2023년 마이크로소프트 보고서의 서두는 "사이버 위협에 대한 통찰력을 공유하고 전세계가 의지할 수 있는 탄력적인 온라인 생태계를 확보하는 데 있어 우리가 직면한 과제에 대해 논의하기 위한 것"이라고 강조하고 "공공부문과 민간부문의 긴밀한 협력이 글로벌 사이버 안보를 개선하고 혁신을 촉진하는 데 매우 중요하다"고 밝히고 있음.[23)]

○ 민간기업의 사이버 위협평가보고서는 대국민 인식 제고 뿐만 아니라 글로벌 인식 지형을 형성하고 사이버 공간의 안보화 방향을 자국에 유리한 방향으로 형성하는 데에도 기여
- 중국 치후360(360公司)은 '미국 관련 APT 분석보고(美相关APT组织分析报告)' 발표, 미국의 사이버 공격이 전 세계 안보우려라고 강조.[24)]

○ 셋째, 사이버 안보 주간 등 대국민 인식 제고 프로그램과 관련하여, 주요

23) Microsoft Threat Intelligence, 『Microsoft Digital Defense Report: Building and improving cyber resilience』 2023.10. p.3.

24) 北晚在线, "《美相关APT组织分析报告》发布：网络攻击属于无差别攻击," 2024.02.07. https://baijiahao.baidu.com/s?id=1790221178046440490&wfr=spider&for=pc (검색일:

국들은 사이버 안보 대국민 인식 제고 위한 활동 프로그램을 시행해오고 있음

○ 미국의 경우 대통령과 의회가 2004년부터 10월을 사이버 안보 인식 월간(Cybersecurity Awareness Month)으로 선포하고, 기술과 기밀 데이터가 점점 더 공유재가 되어가는 위협 속에서 개인들이 온라인에서 스스로를 보호할 수 있도록 돕고 있음.[25)]

- 사이버 안보 인프라 안보국(Cybersecurity and Infrastructure Security Agency, CISA)과 국가사이버안보연맹(National Cybersecurity Alliance, NCA)이 공동으로 사이버 안보 경각심을 국내적으로 국제적으로 제고하기 위해 정부와 산업간의 협력을 이끌고 있음

○ 중국 또한 2014년부터 매해 9월 '국가사이버안보 홍보주간(国家网络安全宣传周)'을 두고 있으며, 국민들의 사이버 안보 인식을 제고할 수 있도록 강의, 전시, 지식보급활동 등 다양한 사이버 안보 위험 알리기 행사 개최

- 사이버안보 홍보주간에는 3대 통신사와 주요은행, 알리바바와 바이두 텐센트 등 40개 이상의 인터넷 회사 및 사이버보안회사 등이 참여
- 홍보주간에 정부와 민간기업의 사이버 안보 협약 등도 추진. 2016년에

2024.03.10.)

25) CISA Cybersecurity Awareness Program.
https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program

는 중국정보안전평가센터(中国信息安全评测中心)와 텐센트가 “국가정보안전방어체계전설(国家信息安全防御体系建设)” 등 4대 영역에서 전면적 협력을 추진하기로 하였음.

- 대체로 홍보주간은 중국공산당 중앙선전부, 중앙사이버안보위원회, 교육부 공업정보화부 공안부 중국인민은행 신문방송총국 공청단중앙 등 다부처가 공동으로 조직. 중앙사이버안전과 정보화위원회가 ‘국가사이버안보 홍보주간 기자회견’ 개최[26)]

○ EU 또한 매해 10월 ‘유럽사이버안보 월간(The European Cybersecurity Month, ECSM)’을 두고, 시민들과 기관들이 교육과 체험을 통해 사이버 안보 인식을 강화할 수 있는 캠페인 실시[27)]

○ 한국 또한 다양한 부처와 관련기관, 시민단체 등이 함께하는 △사이버 홍보주간, △기업 학교 등에 찾아가는 사이버 안보 교육프로그램 △사이버 안보 경각심 제고 위한 다양한 행사와 프로그램 검토 필요

26) 百度百科, “国家网络安全宣传周”
https://baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E5%AE%A3%E4%BC%A0%E5%91%A8/16187822?fr=ge_ala

27) ENISA, “European Cybersecurity Month”
https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month

4. 사이버 안보 국제컨퍼런스 개최 등 글로벌 리더십 강화 및 공공외교 추진 과제

○ 첫째, 1.5트랙 사이버 안보정책 협의 메커니즘 구축 및 교류와 관련하여, 세계 주요국들은 글로벌 사이버 안보 협력을 위한 다양한 레벨의 민관협력의 컨퍼런스 등 개최로 교류협력 및 리더십 강화

- 대만과 미국의 글로벌협력 및 훈련 프레임워크(Global Cooperation and Training Framework, GCTF)는 양국간 공무원 및 전문가 훈련 프로그램을 통해 인태지역 국가 역량 강화를 지원하는 동시에 대만의 다자간협력을 촉진. GCTF 하에 사이버 안보, 전자상거래, 허위정보 등 76개의 주제의 국제워크숍을 조직
- 2024년 5월에는 영국대만사무소와 대만에 있는 미국연구소(American Institute), 일본대만교류협회(Japan-Taiwan Exchange Association(JTEA), 대만외교부, 대만 디지털부가 함께 타이베이에서 정보통신과 사이버안보 회복력 관련 국제세미나 개최. 총 26개국에서 210명의 참가자가 사이버안보, 정보통신 회복력 등 주제로 교류

○ 한국 또한 미국, 영국 등 유사입장국과의 양자간 1.5트랙회의는 물론, 인태지역 국가들의 정부인사, 전문가 등이 참여하는 1.5트랙 국제학술회의 검토

- 사이버 안보 뿐만 아니라 생성AI 규범 등 신흥 사이버 안보이슈 관련 민관협력 거버넌스를 토대로 한국의 전략 도출

○ 사이버 안보 국제컨퍼런스 등 개최, 사이버 위협 동향과 대응, 규범 글로

벌 협력 주도

- 사이버안보학회 등 민간기관과 정부기관이 공동으로 주최하는 '사이버 안보 국제컨퍼런스' 개최. 학자, 연구소, 민간기업이 참여하는 민관협력의 국제 사이버안보회의 연례화
- 사이버 안보 전략과 규범 등 관련 글로벌 트렌드 공유와 주도 뿐 아니라 산업계 협력, 기술협력 등 다양한 융합적 측면에서 논의와 교류 확대 필요

○ 둘째, 사이버 안보 기술, 산업 전시회 등으로 글로벌 사이버 안보 공급망 주도, 시장 확대와 관련하여 정부와 민간이 공동으로 '글로벌 사이버안보 기술산업 전시회' 등 개최하여 세계적인 사이버 안보 관련 기술과 제품 등을 소개하는 연례 행사 검토

- 사이버 안보기술과 산업 주도성, 사이버 안보 기술역량과 네트워크 강화를 위한 민관협력의 거버넌스 구축 가능

5. 글로벌 거버넌스 대응 차원의 민관협력 과제

○ 첫째, ITU, ICANN 등 글로벌 다자협력체 사이버 안보외교 민관협력과 관련하여, ITU는 새로운 디지털 ICT 인프라에 대한 국제 표준 강화, 인공 지능(AI), 클라우드 컴퓨팅, 양자 통신, 전송 네트워크 및 광통신 분야에서 국제 표준의 개발, 적용 및 배포 진전, ICT 시스템 및 네트워크의 일관성, 안정성 및 보안 강화 등 다양한 측면에서 사이버 안보 외교와 밀접

히 연계

- 정부와 기업이 함께 표준제정, 인프라제공, 사이버 안보 강화 등 ITU 차원의 활동 강화, 이를 통한 글로벌 리더십과 공공외교 추구
- 한국은 2017년부터 ITU-T SG17의 의장국을 맡고 있으며, 국제표준회의를 통해 국제표준채택, 기술지침서 제공 등 사이버 보안 국제표준 개발을 위한 활동을 지원하고 있음
- 2007년 ITU는 정보 사회에서 신뢰와 보안을 강화하기 위한 국제협력 프레임워크인 글로벌 사이버 안보 어젠다(GCA, Global Cybersecurity Agenda) 추진. 글로벌 사이버안보어젠다(GCA)는 모든 관련 파트너와의 협업을 장려. 아동 온라인 보호와 같은 이니셔티브를 주도하고, 주요 글로벌 행위자들의 지원과 함께 전 세계 국가에 사이버 보안 솔루션을 배포하고 있음. GCA는 5가지 전략적 기둥-법적 조치, 기술 및 절차적 조치, 조직 구조, 역량 강화, 국제 협력-으로 구성됨[28)]

28) https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

○ 중국은 중국 ICT 이니셔티브와 ITU를 연계하면서 표준주도와 중국 민간기업의 참여와 글로벌 교류를 적극 지원

- 중국은 ITU 심의 연구그룹에 중국 학계와 기업의 참여에 보조금을 지급함으로써 ITU프로세스에 적극적 영향 행사 노력[29)]
- 2022년 화웨이가 ITU의 Partner2Connect-P2C의 디지털 얼라이언스에 가입하고 2025년까지 소외지역에 거주하는 1억2천만명에게 디지털 세계로의 연결성 제공 지원 결정. 화웨이는 파트너국가인 캄보디아 정부 및 대학과 협력해 향후 5년간 전문가들에게 1만번의 교육기회를 제공하기로 한 바 있음

○ 한국은 사이버 안보 역량과 글로벌 리더십 강화를 위해 ITU, ICANN 등 글로벌 다자체제 의제와 협력 주도를 위해 민관협력의 틀을 다양하게 구축할 필요

- 2024년 2월 한국정보통신기술협회가 표준자문을 통해 국내 중소기업이 국제표준제정 및 신규표준과제 채택 성과를 이룰 수 있도록 한 바 있음.

○ 둘째, 다양한 양자, 소다자 협력의 주요 의제로 사이버 안보를 적극 제기하고, 인태지역 사이버 안보외교의 허브로서 역할 모색과 관련하여, 최

29) Brett Schaefer and Danielle Pletka, “Countering China’s Growing Influence at the International Telecommunication Union,” Heritage Foundation, 2022.03.07. https://www.heritage.org/global-politics/report/countering-chinas-growing-influence-the-international-telecommunication

근 사이버 안보가 주요 유사입장국들의 가장 중요한 외교안보 협력 어젠다로 부상함

- 쿼드, 오커스 모두 사이버안보 협력을 주요한 축으로 하고 있으며, 중국이 주도하는 브릭스, 상하이협력기구 등도 사이버 안보 협력을 핵심 어젠다로 하고 있음

○ 한국은 미국은 물론 영국, 호주 등 사이버 안보역량을 갖춘 국가들과의 양자간 사이버 안보 협력 확대와 함께 소다자간 사이버안보협력 메커니즘 구축 필요

- '한미 사이버안보 고위급회의' '한-영 경제·사이버안보대화' 등에 이어 호주 등 사이버 안보역량을 갖춘 유사입장국들과 사이버 안보 양자대화 추진
- 아세안 등 소다자 사이버 안보대화 검토 가능

○ 기술격차, 전략협력의 복잡성 등으로 정부간 사이버안보대화를 본격화하기에 제약이 있는 경우, 비정부 전문가 그룹 혹은 학계간 사이버안보대화 등 토대 구축의 대화 추진 가능

- 2024년 올해 싱가폴에서 개최된 'US-ASEAN Cyber and Digital Dialogue'가 미국 콜럼비아 대학과 싱가폴국립대, 난양공대가 함께 개최한 사이버 디지털 대화는 의견공유와 미래 협력의 경로를 모색하는 대화로 개최.[30)]

30) "2024 US-ASEAN Cyber and Digital Dialogue Kick-Off Session" 2024.06.24.

- 한국 또한 동맹국, 유사입장국과의 정부간 사이버안보대화를 넘어 글로벌남반구 국가들과의 비정부 차원의 사이버 안보대화를 적극 추구 필요. 민간기업과 전문가들이 참여하는 사이버 안보대화의 경우 단순히 외교전략적 목표 뿐만 아니라 기술산업적 기회에도 중요한 플랫폼으로 작용가능

결 론
사이버 안보 국가책략의 과제

연구진 전원

1. 국가적 대응체계 정비의 과제
2. 사이버 보안 국가책략의 과제
3. 사이버 국방 국가책략의 과제
4. 사이버 외교 국가책략의 과제

결 론
사이버 안보 국가책략의 과제

연구진 전원

1. 국가적 대응체계 정비의 과제

① 사이버 안보의 협력 플랫폼과 허브의 역할을 담당하는 사이버 안보 컨트롤타워의 효과적 가동을 통해서 관계부처·기관 및 기업 간 협업을 강화함

- 해당 부처가 각 분야에서 각기 역할을 수행하는 분산적이지만 자율적인 거버넌스 모델을 바탕으로 하지만 이를 조율하는 '메타 거버넌스'의 주체로서 컨트롤타워의 효과적 가동이 중요함
- 기술과 전략, 제도와 법 등 여러 분야를 망라하며 국제협력 및 국제규범 등을 총괄하는 새로운 국가 모델의 발상이 필요

② 사이버 안보의 범부처 공조 체계를 정비하는 노력을 지속할 필요가 있음

- 각 정부 소관 부처별 권한과 책임 및 역할을 정립하는 것이 선행되어야 하며 각 부처의 역할과 책임을 유기적으로 연결 및 조화하는 추진체계를 구축

- 소관 분야별 사이버 안보 활동에 대한 평가를 시행하고 후속 보완 조치를 마련하는 체계를 수립할 필요
- 소관 분야별 업무 수행을 지원하는 제도적 기반 개선

③ 사이버 안보 분야 민관협력 체계를 정비하고 대국민 인식 제고를 위한 노력을 펼칠 필요가 있음
- 위협정보의 공유와 협력의 활성화를 위해서는 민관협력이 핵심이라는 점을 인식하고 공공·민간 영역 간 사이버 위협정보의 공유를 위한 절차와 기준 및 법적 근거를 마련할 필요가 있음
- 사이버 안보위협에 대응하기 위해서는 사회적 공감대의 조성이 필요가 있으므로 국민이 사이버 안보의 중요성과 안전 수칙을 체득할 수 있도록 다양한 체널을 활용해야 함

④ 사이버 안보 외교의 추진체계 정비
- 사이버 안보외교 수행과 관련하여 여러 정부부처가 국제협력 활동 진행 중인데, 이들 사이버 안보외교 업무를 총괄 조정하는 협력체계 또는 이를 모두 아우르는 추진체계의 정비가 필요함
- 기존 부서의 재조정 이외에도 새로운 부서나 기관의 신설도 검토할 필요가 있으며, 사이버 안보외교 분야의 특성을 반영하는 민간(학계) 차원의 1.5트랙 가동도 고려할 필요가 있음

⑤ 사이버 안보 분야 법제도 정비
- 소관 개별 법령에 따라 각 정부 부처가 제각각 분리, 독립 대응하고 잇는 현실을 극복하기 위한 법제도 개선의 노력이 필요함

- 특히 범정부적 사이버 안보 추진체계, 공공과 민간의 소통과 협력, 개인정보 보호, 국제협력 등 사이버 안보 관련 법적 기반 강화를 위한 법제도 개선 필요
- 이러한 과정에서 사이버 안보와 개인정보보호의 조화로운 발전을 담은 내용을 통해 국가와 시민사회 모두의 공감대와 합의를 이끌어 내도록 함

2. 사이버 보안 국가책략의 과제

사이버 정보공유 및 대응역량 강화

① 사이버 정보 수집·분석 및 공유 기반 강화를 위한 책임과 권한, 의사결정체계 및 공유체계 확보 필요

- OEWG의 Global PoC Directory 구축에 적극 참여하되, 공유 정보의 보안성 및 기밀성 유지 방안, 정보 생명주기 전체 보안 고려 필요
- 외교, 정책, 기술 등 다층적 PoC간 정보공유 활동 및 기존 기술협력 체계(FIRST 등)의 중복 가능성 고려, 국가 사이버안보 거버넌스 변경에 따른 CERT간 협력채널, 정보공유채널 등에 대한 재조정 요소 식별 및 조치 시행 필요

② 사이버공격 대응 기준 고도화 및 사이버 위협환경 변화에 따른 우리의 인식, 판단 및 대응 정책과 근거 공개 개시방안 마련

- 구체적이진 않으나, 심각한 위협으로 국가차원의 대응이 필요하다고

생각되는 수준에 대한 개괄적 정책과 근거 개시 필요

- 사이버 사고 발생시 대응 기준 및 국가 대응의 합법성과 근거 확보, 명확한 공격자 식별 기준 마련 필요

③ 공세적 사이버 방어활동 역량 확보 활동에 대한 용어 및 개념 구체화 등 국내 관련 제도 시행을 위한 근거 및 절차 마련

- 공세적 대응과 공세적 방어, 선제적 방어, 억지는 이론적으로 명확한 개념정의에 기반해 전략서에 언급되는 것이, 국가 정책 추진 방향을 명확히 할 수 있음
- 주권개입, 대응조치 시행 등 국제법 및 국내법적 적법성 확보를 위한 노력 필요
- 기술적 활동 강화의 제도적 근거 고려 필요

④ 가짜뉴스 대응, 선거개입 등 영향력 공작 대응방안 확보

- 영향력 공작, 허위정보 유포 및 확산, 가짜뉴스 생산 및 유포, 여론조작 대응을 위한 연구기관, NGO 등 활동 장려, 사회적 인식 및 회복력 강화방안 마련
- AI 등 신기술 활용 대응을 위한 기술적 측면의 연구지원 강화 필요
- 하이브리드 위협 대응을 위한 통합 거버넌스 구축, 제도적 기반 확보 및 국제협력 강화

⑤ AI 도입에 따른 사회적 대응역량 강화를 위한 정책 고려 사항

- 정책지향성 부재, 전문인력의 부족, 학제간 소통 및 문제의식 공유 부재, 정책결정 지원 가능한 생산의 한계, 국가 R&D와의 정합성 부족,

지속적 실행력 부재 등이 지속

- 국가적 이익 달성에 부합하는 정책지향점 수립하고, 범정부 AI 적용과 활용에 관한 미래 시나리오 개발, 전략 및 로드맵 수립 필요

사이버 범죄 및 테러의 예방·대응 역량 제고

① 사이버 범죄-테러 관련 정보수집 및 통합 데이터베이스 구축

- 국가정보원 산하 "국가사이버안보센터 (NCSC: National Cyber Security Center)"를 중심으로 사이버 범죄-테러-에스피오나지 등에 대한 통합 이터베이스 컨트롤타워 설치
- "국가사이버안보센터"를 선도 기관(즉 컨트롤 타워)으로 사이버 안보 관련 정보기관들과 수사기관들을 함께 묶는 정보공동체 구성

② 입법을 통한 수사 권한 강화

- 수사기관의 국내-기반 인터넷 서비스 공급자의 데이터에 대한 접근권한 보장 (미 CLOUD ACT)
- 수사기관을 위해 원격통신사업자와 제조업자가 필요한 감시(Surveillance) 역량을 지원하기 위해 시스템과 서비스를 구축하도록 법적 의무화 (미 Communications Assistance for Law Enforcement Act: CALEA)
- 민간 사업자가 자신들의 IT 시스템에 백도어를 설치하고 이를 수사기관이 활용할 수 있도록 엔크립션(encryption) 키를 수사기관에 제공하도록 법적 의무화 (미 All Writs Act에 따라 몇몇 사례들에서 법원 명령으로 강제)

③ 사이버 범죄에 대한 저항성을 강화하기 위해 일반 국민을 대상으로 한

사이버 보안의식 교육 및 캠페인 추진

- 오늘날 사이버 범죄-테러 피해에 대한 저항성을 의미하는 사이버 역량 격차를 'CPL(Cybersecurity poverty line)'로 부름
- 따라서 CPL을 기준으로 이로부터 상당 정도의 상위 수준을 유지하기 위해서는 일반 국민 대상의 광범위하고 체계적인 사이버 보안의식 교육 및 캠페인이 필요함

④ 사이버 침해 피해에 대한 사이버 보험(cyber insurance) 운용 지원, 제도화

- 랜섬웨어 공격 등에 대한 랜섬(ransom) 지불
- 소송 비용, 수사 비용, 그리고 피해에 대한 구제 등
- 사이버 보험 생태계 구축

⑤ 다자간 사이버범죄 대응 공조협약 가입 추진

- 한국이 사이버 범죄 협약에 가입하게 되면 협약의 국내적 수용을 위한 이행입법을 마련해야 하므로 협약의 절차법 조항과 한국의 형사소송법, 통신비밀보호법 등 관련 조항을 제·개정할 필요 있음
- 가입을 위한 초청은 이후 5년간 유효하며, 한국 정부는 협약 비준을 위한 국내 절차가 완료되면 가입서를 기탁할 예정임
- 협약 가입절차를 완료하기 위해 사이버 범죄 협약의 이행 입법을 마련하여야 함

사이버 안보 기술역량 강화 및 공급망 안보 확보

① 글로벌 다자, 소다자, 지역 및 양자 회의체에서 기술개발협력을 위해 동

맹국들 간 그리고 동지국가들 간 협력이 더 강화되고 있기 때문에 공급망 재편에 대응하기 위한 국내 부처 간 조율체계 구축방안이 필요함

- 기술개발협력 및 공급망 재편은, 수출통제정책, 기술 및 보안 표준 정책의 조화 또는 동조를 필수적으로 수반하기 때문이며, 우리나라는 이들에 대처하는 각각의 부서들이 각자 노력을 해야 하는 한편, 보조를 맞춰가야 함
  · 기술 표준을 순응한다고 하더라도 수출통제정책이 국제적으로 조율되어 있지 않으면, 한국을 통해 기술이 유출될 수 있다고 생각할 수 있기 때문임
- 국제다자협상의 틀이 재편될 때, 적극적으로 참여하여 한국이 여러 첨단 기술 논의에 참여할 수 있도록 해야 하며, 이때 여러 부처간 협력이 전제됨

② 공급망 사이버안보 정책 관련해서 미국과 같은 선진 동맹국들이 앞서 나가고 있기 때문에, 기술 및 제도 차원에서 우리나라도 지속적으로 업그레이드해 나갈 체계가 필요함

- 기대되는 보안 기술이 부족한 경우 또는 유사한 보안 표준을 설정하는 제도가 부재할 경우, 앞으로 데이터 협력도 어려워질 것으로 예상되기 때문에, 사이버안보 기술뿐 아니라, 정책이나 제도 관련 전문가들 양성이 필요함

③ 사이버안보 대응 인재 육성을 위해서는 사이버보안 R&D 투자 확대, 사이버보안 스타트업 지원, 사이버 보안 훈련 및 연습 확대, 민관 협력 및 국제협력 강화, 사이버 보안 전문가 양성을 위한 교육 프로그램 확대 그

리고 대학 및 연구기관과 협력하여 관련 (표준화된)커리큘럼을 개발이 필요함

- 기존에도 인재 육성을 위한 계획이 없었던 것은 아니나 2022년 '사이버보안 전문인력 10만 명 육성 계획'이 나온 계기로, 구체적인 프로그램들을 하나하나씩 실제적으로 이행해 나갈 필요가 있음
  · 이행 경과를 지속적으로 업데이트하며, 달성지표를 만들어 성과를 가시적으로 보이는 것도 필요함

④ 사이버안보 분야의 전략산업화를 위해, 국내 시장의 육성뿐 아니라, 좁은 국내 시장의 한계를 극복하기 위한 글로벌 기업으로 육성할 정부 지원이 필요함

- 2022년 '국가전략기술 육성 방안' 그리고 '국가연구개발사업 예산 배분 조정 결과' 등을 통해 국내 투자 정책이 마련되고 있는 것은 바람직하나, 글로벌 기업으로 육성할 정부의 전략적 지원도 추가될 필요가 있음
  · 기술 강점을 가진 기업을 중심으로, 글로벌 벤처 투자와의 합작을 통해, 넓은 시장에서 성장시키는 방안이 바람직하기 때문에, 정부는 이스라엘 기업들의 성공 사례를 통해, 정부 지원책을 마련할 것이 요구됨.

⑤ 2022년 12대 국가전략기술 지정 등을 통해 신흥기술을 국가적으로 지목한 것은 좋은 방향으로 가고 있으나, 신흥기술에 대한 사이버 위험 관리체계 확립을 위해서는, 선택과 집중을 통해, 부문별로 또는 기술별로 우선 순위를 정하는 것이 더 바람직함

- 선택과 집중은 정치적으로 부담이 되나, 한국이 잘하는 분야를 파악하고 육성하려는 것이 글로벌 경쟁력 차원에서도 바람직함

- 다른 한편, 국가전략기술들 전반적인 사이버위험관리체계의 업그레이드도 소홀히 할 수 없기 때문에, 선진국 사례들에 대한 지속적인 모니터링과 국내 제도의 업그레이드가 필요함
  · 개도국과의 협력을 위한 개도국에 제공할 수 있는 기술 및 제도 개발을 따로 하는 노력도 소홀히 해서는 안 될 것임

3. 사이버 국방 국가책략의 과제

사이버 군사전략과 동맹협력

① 사이버 동맹의 전략적, 실질적 발전을 위해서는 전통적 상호방위체제의 포괄적, 전환적 협력을 위한 동맹협력 목표가 재검토
- 초국경적, 초영역적 공간인 사이버 영역에 있어서 동맹협력은 전통적 동맹체제의 상호운용성의 본질적인 변화를 수반함
- 네트워크 보안은 물론 방어적·공세적 사이버 작전에 있어서 초영역적, 초국경적 협력의 심화를 위해서는 전략적 수준을 넘어, 작전적, 전술적 협력을 심화
- 인공지능, 빅데이터, 클라우드 등 국방체계의 디지털 전환에 따라 디지털 리스크 대응 및 디지털 상호운용성을 포함하는 장기적으로 통합적 상호운용성을 위한 단계적 동맹협력 과제가 검토되어야 함

② 한미 사이버 동맹은 사이버 공간에 대한 북한의 비대칭 위협에 대응하는 한편, 북핵위협을 억지, 방어하는 비대칭 우위전략으로서 통합적 사

이버 협력

- 디지털 전환에 비례하여 디지털 리스크 및 사이버 취약성이 증가하며, 이를 비대칭 사이버 위협수단으로 활용하는 북한의 전략에 대응해야 함
- 반대로 사이버·전자기 영역을 통합에 기반하는 다영역전략과 작전은 북한에 대한 전략적 우위수단으로 한미동맹 협력을 발전시킬 필요가 있음

③ 과제 3: 한미 사이버 동맹이 전통적 확장억지력을 보완, 강화하는 통합적 억지력의 기반이 되기 위해서는 전략적, 작전적, 제도적, 기술적 상호운용성의 동시적, 통합적 협력의 심화 추진

- 사이버 동맹의 전략적, 작전적, 제도적, 기술적 상호운용성의 기반으로서 사이버 상호운용성을 위해서는 ⑴ 통합적, 다차원 사이버 전략목표에 따라, ⑵ 궁극적으로 디지털 상호운용성의 심화를 위한 기술, 공급망, 전략, 작전 차원의 협력이 심화되어야 하며, ⑶ 디지털 로우-하이 믹스개념에 따라 전략, 작전, 부대차원의 동맹협력 목표가 단계적으로 추진될 필요가 있음

④ 과제 4: 한미 사이버 동맹기반 사이버 집단안보 참여, 주도해야함

- 개방성과 상호운용성은 디지털 기반 군사체계의 효과성은 물론 초국경성, 초영역성을 가지는 사이버 위협에 대응하는 기반임
- 한미동맹은 물론 전략적 이해를 공유하는 국가와 사이버 군사기술, 군사전략, 무기체계 등 포괄적인 사이버 안보 혁신 네트워크를 구축, 주도할 필요가 있음

⑤ 과제 5: 인재양성은 사이버 동맹 및 사이버안보 혁신네트워크의 출발점임

- 국내적으로 민관군산학연을 통합하는 사이버 인재양성과 더불어 대외적으로 동맹국, 협력국과 함께 다자적인 인재양성 기반을 구축할 필요가 있음

사이버전 수행역량 강화와 공세적 방어

① 전쟁 패러다임 변화를 반영하여 사이버전 전략과 전술, 수행체계 및 기술을 획기적으로 발전시키고 고도화

- 미중 군사혁신 경쟁과 최근 전쟁에서 드러난 전쟁 패러다임 변화를 반영하여 사이버전 전략 및 전술 수행 체계 재편이 긴요함
- 재편된 사이버전 전략, 전술 이행에 필요한 핵심 기술의 단기적, 중장기적 확보를 위해 기술 고도화 전략의 구축 및 체계적 이행 필요

② 새로운 전쟁 패러다임을 반영하여 사이버전 역량을 통합적으로 운용할 수 있는 작전 수행체계 구축

- 현대 전장은 다영역 공간이며 지상, 해상, 공중, 사이버, 우주, 전자기장 영역에 존재하는 모든 전력을 동시, 통합적으로 활용하는 것이 승리의 요체
- 사이버 방어, 공격 작전은 특정한 조건 하에서 단독으로 시행될 수 있으나 우주, 전자기장 작전과 동시에 시행되어 상호 상승효과를 강화해야 하며 지상, 해상, 공중 작전과의 긴밀한 연계 속에서 시행되어야 함

③ 공세적 사이버 방어 및 대응 개념의 정립을 통해 전평시 사이버 안전과 전략적 우의의 달성 및 보장

- 향후 사이버 공격은 더욱 은밀한 방식, 다양한 규모로 감행, 이에 대해 충분한 방어와 대응이 이루어지지 못할 경우 국가 안보 역량의 심각한 저하가 불가피
- 사이버 공격의 조기 감지 및 신속한 대응은 국가안보의 기반이 될 것인 바 조기 경보 체계의 지속적인 발전과 확대가 긴요
- 사이버 공격이 감지, 식별되는 경우 관련 체계 및 역량 운영 기관에 정보를 공유, 다양한 수준과 단계에 따른 대응으로 적이 공격을 확대하지 못하도록 해야 함

④ 다영역 작전 수행을 위해서는 사이버전 지휘통제체계 수립이 핵심적 근간이며 이를 위해 '사이버 전장 가시화', '합동 전장 가시화 체계' 구축 및 통합이 필요

- 사이버 지휘통제체계 수립은 현대 및 미래전의 기본 패러다임인 다영역 작전 수행의 근간이 되므로 미래 지향적인 지휘통제체계 수립을 단기적으로 뿐 아니라 중장기적 관점에서 체계적으로 구축해 나가야 함

⑤ 사이버전 무기체계의 체계적 개발 및 전력 체계와 핵심 기술 고도화 추진

- 미래 첨단 기술을 반영한 사이버전 신 무기체계 개발 노력을 지속해야 하며 전력 체계 발전도 추진해 나가야 함
- 이와 관련된 핵심 기술 고도화를 위해 국방 사이버 무기체계 개발 생태계를 구축하고 관련 국제적 협력도 고도화해 나가야 함

사이버 불법 활동·영향력 차단 및 사이버 기반 조성

① 북한의 경제적 불법행위를 능동적으로 차단하기 위한 카운터해킹 역량 강화 및 유관기관 간 협력 보장을 위한 제도 개선

- 가상화폐 탈취 및 세탁 과정에서 적의 취약점을 역공격할 수 있는 전문 화이트 해커 양성 체계 강화
- 사이버 상의 경제적 불법행위에 대한 민관, 유관기관 간 원활하고 견고한 협력· 소통 채털 구축 등 대응 인프라 법제 개편 및 규제 강화기능

② 북한의 사이버 영향공작의 징후, 탐지·경고 및 평가 역할을 주도할 조직 체계 신설 및 기능별 임무 수행 및 허위정보 확산 방지를 위한 법제 개선

- 선거 위협 등 '사활적 문제'에 한해 포괄적이고 종합적인 대책으로서 , 사활적 문제 한해 외국인 간첩법과 사이버 허위정보 확산 금지법 적용 논의 필요
- '허위정보의 위험층위' 기준원칙, 규정을 마련, 위중한 가짜뉴스에 대해 징벌적 손해배상제도를 적 등, 능동적 조치 시행 및 사회의 '정보 리터러시(Information Literacy)' 강화

③ 대북 사이버 제재 실효성을 높이기 위한 공조체계 구축 및 사이버 제재 대상 북한 해커에 공세적 조치를 위한 정보·법집행 기관의 적극적 참여 보장 제도 정비

- 국제사회의 책임귀속 논의에 적극 참여하고, 서방, 동류국가들과 탈린 매뉴얼 개정을 통해 책임귀속을 위한 기술적 법제적 기준을 구체화하는데 적극 참여

- 특히, 제재 대상인 북한 기관·해커가 보유한 자산에 대한 동결 및 몰수 조치를 강행할 수 있는 입법적 조치를 고려할 필요
  · 북한 해커 포함한 국제 해커 조직·단체에 대해 책임귀속을 실행할 수 있는 기술적 정보 수집·제공, 미국 정보기관 및 법집행기관과 함께 처벌 기소할 수 있는 활동 강화

④ 북한 사회의 디지털 억압실태 개선을 위한 재정지원 기반 마련 및 북한 통제를 우회하여 침투할 수 있는 전통 수단과 신기술 개발 병행
- 정보통제 대응 기술개발을 위한 다양한 프로젝트를 지원 중인 미국 사례 참조, 북한 사회의 디지털 억압 개선을 위한 재정지원 기반 마련
- 북한 내부 정보화·네트워크화 수준과 외부의 기술적 침습도를 종합 고려한 신기술 개발 및 非네트워크워크 기술개발 병행
  · 북한의 내외망 분리, 별도운영체제, 전자서명체계 등을 초월하거나 우회한 침습적 기술력 확보 가능 여부에 대한 기술공학적 검토 시행
  · 국경 전파방해 차단 및 국가망 접속 인증체계 교란기술, Space-X사 직접통신(D2D) 위성과 같은 혁신적 차세대 통신 네트워크 기술 개발 추진

⑤ 급변사태 등을 고려한 북한 사회의 디지털 환경 실태 진단 및 활용방안 탐색
- 급변사태, 비핵화 진전을 고려한 북한 개방 시나리오는 언제든지 발생할 수 있으므로 국면 전환 하에서 새로운 대북 진출을 위한 추진 로드맵 마련
- 북한의 디지털 기기와 서비스를 경험하며 인터넷 자유도에 대한 인식

을 가지고 있는 바, 전면차단의 불편성을 강조하여 정권불만을 유도할 수 있는 방안 탐색

- 공세적 관점에서 우리의 대북 사이버 역량을 강화하기 위해 북한 사회계층별 디지털 환경실태 조사 프로젝트 및 활용 인식 조사 연구 수행
- 일방적 지원이 아닌 남북 '이익공유'에 기초한 북한 인프라·자원 등 개발 및 관련 자료의 디지털화 기반 검토
  · 기존 북한 개발은 남한의 일방적인 지원에 기초한 측면이 비판적으로 제기되었는 바, 북한 개발(특히 자원개발 등)에 따른 이익을 남북이 공유하는 방향으로 추진 필요

4. 사이버 외교 국가책략의 과제

사이버 안보 동맹협력 및 소다자 협력

① 향후 한국은 미국과의 사이버 동맹 훈련을 확대시켜 인태지역에서의 시그니쳐 훈련(가칭 '인태 사이버 연대 훈련')을 미국과 함께 주도해야 함

- 전 세계 최고의 사이버 역량을 보유한 미국, 호주, 한국과 사이버 위협의 최대 진원지인 러시아, 중국, 북한이 모두 위치한 인태지역은 한국의 민주주의 우호국 및 유사입장국 간 사이버 안보 협력을 통해 역내 안보 증진 효과를 기대할 수 있는 지역.

② 한국은 인태지역 소다자 협의체와 함께 '전략커뮤니케이션센터(strategic communication center)' 혹은 '정보상황실(information situation room)/정보

퓨전센터(information fusion center)'를 버추어 플랫폼(virtual platform)의 형태로 구축해야 함.

- 이러한 플랫폼을 통해 러시아, 중국, 북한으로부터의 사이버 위협 정보와 국가 배후 허위조작정보를 실시간으로 공유하고 인태지역에 합동주의보와 같은 공통의 메시지를 발신할 수 있음.
- 이러한 플랫폼에 합동훈련 결과나 공동 연구결과 및 공동 행사 등의 정보를 담은 인태지역의 사이버 안보 협력 성과를 게시하여 역내 청중과 미디어에 알리고 홍보할 수 있는 창구로 활용할 수 있음.

③ 한미일 사이버 안보 협력을 위해 3국의 공동 목표와 비전을 담은 문건 작성 및 발표하여 3국의 국내 정치의 변동에 영향 받지 않는 지속성 있고 일관된 협력의 틀을 구축해야 함.

- 그러한 문건에는 ▲한미일의 사이버 안보 협력이 인태지역과 세계안보에 어떻게 기여할 수 있는지, ▲한미일이 현재 어떤 공통의 사이버 위협에 직면해 있는지, ▲한미일의 사이버 역량이 함께 투사될 경우 인태지역에서 어떤 작전을 추진할 수 있는지, ▲한미일이 사이버 안보 분야에서 이루고자하는 공통의 비전과 목적은 무엇인지를 담을 수 있음.

④ 한국은 사이버 위협을 포함한 다양한 하이브리드 위협에 대해 유럽과 동질적인 이해와 협력을 도모하는 '유럽 하이브리드 위협 대응센터(European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE)'와의 협력을 추진해볼 필요가 있음.

- Hybrid CoE는 하이브리드 위협 대응에 있어서 NATO와 EU간 전략적 토론과 훈련을 촉진하고 위협 대응의 모범사례를 개발하며 연구결과

를 역내에 공유하는 기능을 담당하고 있고, Hybrid COE가 주최하는 'Cyber Power Symposium on Hybrid Conflict and Warfare(CPH)'에 2023년 일본, 호주, 우크라이나 등이 참여했고, 이 심포지엄에서는 사이버뿐 아니라 사이버 위협과 하이브리드 위협의 연결성, 사이버 방어 차원에서의 인지전과 하이브리드전의 관계성, AI 기술과의 관계 등을 논의한 바 있음.

⑤ 한국은 유럽의 사이버전, 하이브리드전, 인지전에 대한 접근법이 구체적으로 만들어지는 NATO전략커뮤니케이션센터(NATO Strategic Communication Centre of Excellence, StratCom COE)에 인력을 파견하고 다양한 연구를 함께 추진할 필요 있음.

- NATO의 허위조작정보 대응 및 인지전 관련 연구는 NATO CCDCOE와 NATO StratCom COE을 중심으로 진행되고 있으므로 우리의 NATO 의 인지전 대응 논의에의 참여 자체가 어려운 일이 아닐 뿐 아니라 NATO는 한국의 참여를 굉장히 환영할 가능성이 매우 높음.

사이버 안보의 국제규범 외교 및 지역협력 외교

① 유엔에서의 사이버안보 규범 논의에 대한 효과적 대응 전략 확립 필요

- 글로벌 사이버안보 규범 무대로서의 유엔의 한계를 분명하게 고려하면서도, 한국의 사이버안보 외교의 지평을 미국과 유사입장국과의 협력을 넘어 확대하는 공간으로 모색할 필요성이 있음.

② G7과 나토를 중심으로 하는 사이버안보 규범 확립에 적극적으로 관여할 전략 확립 필요

- 미국, 유럽, 일본을 비롯한 선진국이자 유사입장국들이 G7과 나토를 중심으로 사이버안보 규범을 확립하려는 최근 흐름에 적극 부응하여, 현재 G7과 나토의 협력국 차원의 한국의 위상을 실질적인 주도국가 수준으로 제고하는 노력이 필요함.

③ 사이버안보의 글로벌 규범 확립에 대한 국제기구 및 1.5트랙 대화에 있어서 사이버 공간의 자유주의적 가치를 적극적으로 주도하는 전략 확립 필요

- ITU와 같은 국제기구 및 물론 민주주의 정상회의 등 글로벌 차원의 다자적 논의 공간에서 사이버 영역에서 추구되어야 할 자유주의적 가치에 대한 한국 정부의 자세를 적극적으로 드러내는 노력이 필요함.

④ 한미협력과 공진화하는 사이버안보의 지역협력 전략 확립 필요

- 한미협력 및 유사입장국과의 협력을 한국 사이버안보 외교의 기축으로 하는 가운데, 글로벌 사우스의 대두 및 미국으로부터의 불확실성 증가의 조건 속에서 동아시아 지역협력을 사이버안보 외교에서 강화할 노력이 필요함.

⑤ 한국의 ODA 전략에서 사이버안보 분야의 협력의 강화 전략 확립 필요

- 신흥국에 대한 ODA의 중요성이 갈수록 증가하는 가운데, 사이버안보 정책 수립, 법제도 형성, 기술 도입 및 인력 양성에 대한 신흥국의 관심이 증가하는 여건을 고려하여, 사이버안보 분야를 한국의 ODA에서 비중을 강화하는 정책 변화가 필요함.

사이버 안보/외교와 민관협력

① <사이버 안보 민관협력 종합 전략서> 수립, 중장기 로드맵과 구체적 이행과제 발표 필요

- 한국형 사이버 안보 민관협력(Public-private partnerships, PPPs) 종합전략을 담은 보고서 마련 필요. 실질적으로 어떠한 분야에서 어떻게 협력해야 하는지에 대한 종합적 검토와 구체적 이행전략 제시

② <사이버 안보 민관협력 프로젝트, 플랫폼> 구축. 민간기업, 전문가 참여 촉진

- 영국의 'Industry 100 이니셔티브'와 미 국토안보부의 AEP와 같이 다양한 부처와 광범위한 민간기업, 전문가들이 함께 참여하는 연간프로젝트 등을 통해 위협 공유와 위협대응을 위한 인프라 확산, 기술역량 제고, 사이버안보 프로그램 등 다양한 측면에서 협력 제도화 필요

③ <글로벌 사이버 안보외교 민관협력> 강화

- 호주의 사이버 역량 구축 프로그램인 사이버 및 핵심 기술 협력 프로그램(CCTCP)은 인도 태평양 전역에서 사이버 회복력 개선 추진. 최근 주요국 기술대사직(Tech Ambassador) 신설, 글로벌 빅테크기업에 대한 reach out과 사이버안보 협력 주력하는 기술외교 확대
- 한국 또한 정부-해외민간기업, 민간기업-해외정부 등 다양한 측면에서 사이버 안보외교 확대강화 필요. ITU 등 글로벌 거버넌스 관여도 민관협력 방안 수립 필요

④ <대국민 사이버안보 인식제고를 위한 민관협력> 강화

- 사이버안보는 전사회적 접근("whole-of-society approach")이 매우 중요하다는 점에서 전국민, 전사회의 관심과 인식제고, 공동대응의 문화와 생태계 구축을 위한 민관협력 필요
- CISA의 사이버 안보 인식 제고 프로그램(Cybersecurity Awareness Program), EU사이버안보국 "AR-in-a-BOX" 패키지 등 참고, 민관협력의 사이버 안보 인식제고 프로젝트 추진 필요
- 미 대통령과 의회가 2004년부터 10월을 사이버 안보 인식 월간으로 선포한 미국의 사례 등 참고, 사이버 안보 주간 등 대국민 인식 제고 활동 강화

⑤ 사이버 안보 국제컨퍼런스 개최 등 글로벌 리더십 구축위한 민관협력

- 세계 주요국들은 글로벌 사이버 안보 협력을 위한 다양한 레벨의 민관협력의 컨퍼런스 개최로 교류협력 및 리더십 강화. 한국 또한 민관이 함께 참여하는 미국, 영국 등 유사입장국과의 양자간 1.5트랙회의는 물론, 인태지역 국가들의 정부인사, 전문가 등이 참여하는 1.5트랙 국제학술회의 추진 필요

2024 KACS 스페셜리포트

사이버 안보 국가책략:

국제정치학의 시각

연구책임자: 김상배(서울대)

공동연구원: 김소정(국가안보전략연구원)
윤민우(가천대)
유인태(단국대)
윤대엽(대전대)
설인효(국방대)
윤정현(국가안보전략연구원)
송태은(국립외교원)
이정환(서울대)
차정미(국회미래연구원)

연구보조원: 신승휴(서울대)

발 간 일: 2024년 12월 31일