KISA INSIGHT

DIGITAL & SECURITY POLICY

2023 VOL. 1

미국·EU·영국 등의 사이버보안 전략 분석 및 시사점

한국인터넷진흥원(KISA)
김도원, 하병욱, 김성훈

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

KISA INSIGHT
DIGITAL & SECURITY POLICY
2023 VOL. 1

미국·EU·영국 등의 사이버보안 전략 분석 및 시사점

CONTENTS

『KISA Insight』는 디지털·정보보호 관련 글로벌 트렌드 및 주요 이슈를 분석하여 정책 자료로 활용하기 위해 한국인터넷진흥원에서 기획, 발간하는 심층 보고서입니다. 한국인터넷진흥원의 승인 없이 본 보고서의 무단전재나 복제를 금하며 인용하실 때는 반드시 『KISA Insight』라고 밝혀주시기 바랍니다. 본문 내용은 한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

[작성]

한국인터넷진흥원(KISA) 미래정책연구실 정책개발팀

김성훈 팀장	061-820-1426	shkim@kisa.or.kr
하병욱 책임연구원	061-820-1288	ha@kisa.or.kr
김도원 선임연구원	061-820-1228	dowonkim@kisa.or.kr

요 약

| 최근 글로벌 주요국은 디지털 환경변화 및 패러다임 변화에 적시 대응할 수 있는 국가 차원의 사이버보안 전략을 지속해서 발표

[표 1] 최근 3년간 주요국 사이버보안 전략 및 핵심 키워드

국 가	주요 내용
 미국	• 국가안보전략(National Security Strategy, '22. 10.) – 국가 경쟁력 강화(산업 현대화, 혁신 및 인재 투자), 글로벌 협력(외교, 포괄적 연합, 풍요 증진), 사이버·기술·기후·에너지·경제·무역 보안 등 • CISA 전략계획 2023~2025(CISA Strategic Plan 2023~2025, '22. 9.) – 사이버 공간의 방어 및 복원력, 주요 기반시설 및 네트워크 보호, 사고 대응 능력 향상, 정보 공유의 강화, CISA 조직 통합 등
 EU	• 사이버방어정책(EU Policy on Cyber Defence, '22. 11.) – 회원국 간 강력한 사이버 방어 공동 대응, 민간 커뮤니티 공조 강화, 사이버 복원력 강화 사이버 방어 핵심 기술 개발, 사이버보안 동맹 강화 등
 영국	• 국가사이버전략 2022(National Cyber Strategy 2022, '21. 12.) – 사이버 생태계 강화, 사이버 복원력, 사이버파워에 필수적인 기술, 사이버보안 글로벌 리더십, 사이버공간의 국가보안 강화
 프랑스	• 국가전략 2022(Nationale stratégique 2022, '22. 11.) – 강력하고 신뢰할 수 있는 핵 억지력, 단합 및 회복력, 프랑스 산업의 전쟁 지원 노력, 최고 수준의 사이버 복원력, 프랑스의 동맹 위상 등
 독일	• 사이버보안전략 2021(Cybersicherheitsstrategie für Deutschland 2021, '21. 9.) – 디지털 환경에서의 자기결정권, 국가와 기업의 사이버보안 공동 대응, 지속 가능한 국가 사이버보안 아키텍처, 국제 사이버보안의 적극 역할
 일본	• 新 사이버보안전략 2021(サイバーセキュリティ戦略 2021, '21. 9.) – 디지털 대전환과 사이버보안, 사이버 공간 전체의 안전 확보, 사이버 공격에 대한 안전 확보 및 동맹·우방국 협력 강화

I

미국·EU 사이버보안 전략

1-1. 미국, 국가안보전략 (National Security Strategy, '22. 10.)

| 국가안보전략은 향후 10년간 미국의 국가 이익 증진 및 경쟁력을 확보하고 향후 글로벌 공동 도전 과제 대응을 위한 방향성을 제시

• 전략에서는 **사이버보안**을 **통합억지 개념**으로 다루고 있으며, **사이버범죄 및 사이버위협에 대한 복원력 확보**를 위해 **국제협력을 통한 공동 대응**을 강조

| PART 1. 미래를 위한 글로벌 경쟁 환경

• 비전

- 탈냉전 이후 새로운 세계 질서 형성을 앞두고 강대국 간 경쟁이 진행 중이며, 자유·안전·개방·번영을 위한 미국의 리더십 발휘 필요
- 기후 변화, 식량 불안, 전염병, 테러, 에너지 부족, 인플레이션 등 글로벌 도전 과제 대응을 국가 및 국제 안보의 핵심으로 인식하고 각국 정부가 협력해야 할 시점에 직면

• 역할

- 미국의 국익 추구 및 안전 보호, 세계의 민주적 가치 실현·뒷받침, 국제협력을 통해 자유롭고 개방적이며 안전하고 번영하는 보다 나은 미래 달성을 도모

• 민주주의 경쟁의 본질

- 자유롭고 개방적이며 번영하고 안전한 세계에 대한 미국의 비전을 공유하며 자유와 존엄성을 추구하는 국가들과 연대
- 권위주의적 통치와 수정주의적 외교 정책을 펼치고, 민주적 정치 과정을 적극적으로 훼손하고, 강압과 억압을 위해 기술과 공급망을 악용하는 러시아 및 중국과의 경쟁

• 경쟁 시대에 협력을 통한 과제 해결

- 민주주의와 전제정치 간의 경쟁 심화는 존재하지만 모든 국가에 영향을 미치는 공동의 도전 과제 또는 초국가적 도전 과제의 해결 필요
- (기후 변화) 모든 국가에 해당되는 잠재적·실존적 문제이며, 기상 이변과 식량 불안, 인류 건강 위협, 분쟁과 대량 이주, 에너지 경쟁 등의 원인으로 작용
- (전염병) 코로나19와 같은 팬데믹 창궐, 공급망 붕괴, 불평등 확대 등의 결과 초래

| PART 2. 미국의 강점에 대한 투자 강화

• 국가 경쟁력 강화

- (산업 현대화 및 혁신·투자) 민간 산업 부문과 개방된 시장은 국가 경쟁력과 혁신의 원천이지만, 시장만으로는 급속한 기술 변화, 글로벌 공급망 붕괴, 비민주주의 국가의 반시장 행위, 기후 변화 대응이 어려우며, 강력한 산업 및 혁신을 유도하는 전략적 공공 투자가 동반되어야 하는 상황

※ ▲교통·광대역·수자원·에너지를 비롯한 물리적 인프라 시설에 대한 투자 단행, ▲반도체 산업 활성화를 위한 「반도체과학법」 발효, ▲'30년까지 탄소 배출량의 40% 감축을 위한 「인플레이션 감축법」 제정, ▲사이버 공격에 대한 복원력 강화 도모 등

- (사람에 대한 투자) 가장 영향력 있는 공공 투자는 인재에 대한 투자이며 상향식 경제 강화를 위해 인력, 인재, 노동력 대한 공공 투자 시행

※ ▲저렴한 의료·보육 서비스의 평등한 접근 확대, ▲장기 직업 훈련 및 스킬 구축, 고품질 교육·훈련 제공, ▲노조 및 단체교섭 뒷받침, 일자리의 질 개선 등

- (민주주의 강화) 미국의 민주주의는 전 세계 사람들의 영감의 원천이었으며 정부 시스템은 법치를 존중하고 개인의 평등과 존엄성을 보호하기 위해 노력하며, 미국의 민주적 절차에 대한 방해를 방어하고 억제하기 위해 방해에 대해 단호한 행동 실시

※ 민주주의에 입각한 평등과 법률, 정책 기관, 포용성 등

• 강력한 연합을 구축하기 위한 외교 실시

- (산업 현대화 및 혁신·투자) 북대서양조약기구(NATO), 미국-EU 무역기술위원회, 미국-영국-호주 동맹 오커스(AUKUS), 인도-태평양 지역 'Five Eyes' 등을 통한 안보 협력 증진
- (포용적인 연합) 타국 주권과 영토 존중, 공정한 경제적 교류 수단 제공, 공동 번영 촉진 등을 도모하는 모든 국가와의 포괄적인 연합 구축을 뒷받침
- (풍요 증진) Covid19, 권위주의 국가 등장, 기후 위기, 식량 부족, 에너지 가격 급증 등에 대응하기 위해 지역별 동맹국 또는 우호국과 협력하여 공동의 도전 과제에 대응

• 군의 현대화 및 강화

- 세계 최고의 전투력을 가진 미국은 국익을 지키기 위해 무력사용을 주저하지 않을 것이나 무력은 최후의 수단이며 민주주의 가치와 법률에 부합하고 미국민의 동의를 얻을 때 사용
- 미국의 강점을 살린 **통합 억제의 접근방식을 사용**할 것이며 군을 지속 가능, 생존 가능하며 민첩하고 대응력 있게 현대화하여 전투능력을 향상

☞ 중국, 러시아 및 기타 국가의 침략과 위협적인 행동에 대한 대응은 더 이상 **재래식 군대**와 **핵 억지력에만 의존할 수 없음을 인지**하여 통합적인 억제 전략 수립

[표 2] 통합 억제의 접근방식

구분	내용
1. 도메인 간 통합	- 경쟁국들의 전략이 **군사(지상, 항공, 해상, 사이버 및 우주) 및 비군사(경제, 기술 및 정보) 영역**에서 다양하게 수립되므로 **영역 간 통합** 실시
2. 지역 간 통합	- 경쟁국들이 확장된 야망과 성장하는 능력을 결합하여 주요 지역과 본토에서 미국의 이익을 위협하므로 지역 간 통합 실시
3. 충돌 범위 전반에 걸친 통합	- 경쟁국들이 무력 충돌 직전의 선을 넘지 않으면서도 미국의 중요한 이익을 해체는 방식으로 갈등을 일으키지 못하도록 충돌 범위 통합 실시
4. 미국 정부 전반의 통합	- 외교, 정보, 경제에서 안보지원 및 전력 태세 결정에 이르기까지 미국의 모든 이점을 적절히 활용하기 위한 정부 전반의 통합 실시
5. 동맹국 및 파트너와의 통합	- 동맹국과의 상호 운용성 및 공동 역량개발, 협력계획, 외교의 조율, 경제적 접근 방식에 대한 투자를 통한 통합 실시

- **신흥기술이 전쟁을 변화시키고 새로운 위협**이 됨에 따라 사이버 및 우주 영역의 대응 능력, AI·양자 시스템을 포함한 **다양한 최첨단 기술에 투자**
- 핵 억지력은 미국의 최우선 과제이며 안전하고 효과적인 핵무력은 동맹국과 파트너를 보호하므로 잠재적인 적들에 대응하기 위해 전 세계에 핵 군 배치

PART 3. 글로벌 우선 대응 과제

• 중국과의 경쟁우위 및 러시아에 대한 제약

- (중국) 중국은 국제 질서를 재편하려는 의도와 이를 실현할 경제적, 외교적, 군사적, 기술적 힘을 가진 유일한 경쟁자이며 세계를 주도하는 강국이 되려는 야망을 보유

- 미국의 동맹국과 파트너들이 중국이 가진 야망과 강압에서 벗어나 자주적인 결정을 내릴 수 있도록 투자, 개발, 시장 제공을 위해 노력

※ 대만 해협 전역의 평화와 안정 유지, 홍콩 자치권, 티베트 인권 침해, 반인도적 범죄 제재 등

- (러시아) 러시아는 국제 질서의 핵심 요소를 뒤집는 제국주의 외교 정책을 추구하고 있고 우크라이나 침공, 미국 정치에 대한 개입 등 민주주의를 훼손하고 분열을 추구

- 미국은 유럽 전역에서 NATO, 유럽연합과 함께 러시아에 맞서고 공동의 가치를 위해 연합하였으며 러시아의 위협에 대한 집단적 회복력 강화를 위해 집중

• 공동 도전과제에 대한 협력

- (기후·에너지 안보) ▲청정에너지 전환 투자로 양질의 일자리 창출과 미국 산업 경쟁력 강화 ▲연방·주 정부의 대응 및 복원력 강화 ▲EU와의 철강 협정 등 주요 업종별 배출 감축을 위한 글로벌 협력 증진 ▲에너지 안보 달성을 위한 세부 조치 추진 등

- (펜데믹과 바이오 안보) ▲조기 경보·질병 감시 등을 통한 바이오 리스크 대비, 의약품 개발·제조·유통 가속화, 안전한 생명공학 기술 발전·제조 증진, 의료 혜택 품질·접근성 개선 ▲세계보건기구(WHO) 산하 코벡스(COVAX)를 통한 세계 보건 안보 지원 및 협력 강화

- (식량의 불안정) 세계식량계획(WFP)의 최대 기여자로서 식량 위기를 겪는 나라를 위해 장기적으로 다자기구, 비정부기구, 현지 파트너 등과 협력하여 글로벌 식량 안보 강화를 도모

- (무기 통제 및 비확산) 대량 살상 무기, 핵무기 등의 확산을 방지하기 위해 동맹국 및 파트너, 시민사회, 국제기구와 협력하여 통제 및 비확산 메커니즘을 강화

※ 핵확산방지조약, 포괄적 실험금지조약기구, 국제원자력기구, 유엔기구 등

- (테러) 테러 방지를 위해 전 **세계의 신뢰할 수 있는 동맹국 및 파트너에 대한 협력과 지원**을 늘리고 '미국 주도 → 파트너 지원' 전략에서 **'파트너 주도 → 미국 지원' 전략**으로 전환

※ 파트너의 법 집행, 사법 시스템 강화, 위협 정보 공유 개선, 국경 보안 강화 등

☞ **다국적 범죄 조직**(TCOs, Transnational criminal organizations)이 일으키는 범죄는 글로벌 문제를 증폭시키는 동시에 많은 피해자를 양산하므로 이를 퇴치하기 위한 방안 마련 필요

- **사이버 공격**, **사이버범죄**, 마약밀매, 자금세탁, 절도, 인신매매, 사기, 부패, 불법 채굴 등 다양한 불법행위는 공공의 안전과 건강을 위협

☞ 미국은 **외교, 금융, 정보 및 기타 도구와 법 집행의 중요 업무를 통합**하고 동맹국 및 파트너와 협력하여 **초국가적 범죄의 억제 노력 강화**

- 다국적 범죄 조직의 공급망과 재정을 방해하고 국제기구를 통해 마약 등 불법 화학 물질을 다루지 못하도록 방지

• 글로벌 규범 형성

- (기술) 미국과 같은 생각을 가진 동맹국 및 우호국과 민주주의 국가들이 협력하여 국가의 안보, 번영의 가치를 향상 시키는 미래 신기술에 대한 발전을 촉진

※ 마이크로 전자공학, 최첨단 컴퓨팅 및 양자 기술, AI, 생명공학, 첨단 통신, 청정 에너지 기술 등

- **(사이버공간의 보안) Quad 등 동맹국 및 파트너와 긴밀히 협력**하여 **사이버 복원력을 빠르게 개선**하고 공격에 **신속하게 대응 할 수 있는 집단적 역량을 구축**

- **국가 기능 또는 중요 인프라를 방해하는 행위**를 포함한 **사이버 공간의 적대적인 행위**에 대해 **모든 국력과 도구를 사용하여 단호하게 대응**

※ 국제법이 오프라인과 마찬가지로 온라인에도 적용된다는 것을 인정하는 책임 있는 국가 행동 프레임 워크 준수 촉진

- (경제·무역) 기존 글로벌 경제·무역 규범이 중국 등 비시장적 행위자로 인해 훼손되고 기후위기·디지털 무역 등의 사안을 반영하지 못하고 있으므로, 미국 노동자와 기업, 동맹국, 파트너가 번성할 수 있는 공평한 경쟁의 장을 수립하기 위한 규범 정립 협력을 강화

- (인질, 억류) 정부, 정권 등이 미국인을 인질로 잡거나 부당하게 구금하는 것을 저지하기 위해 2022년 7월 레빈슨법(Levinson Act)을 발효하고 비인도적 관행에 반대

| PART 4. 세계 지역별 전략

• 전 세계 국가 및 국민과의 협력

- 안보, 번영, 자유는 어느 때보다 연결되어 있으며, 우리의 미래를 보장하기 위해 파트너와의 협력 필요

- 자유롭고 개방적인 인도-태평양 촉진, 유럽과의 동맹 심화, 서반구에서 민주주의와 공유 번영 촉진, 중동의 긴장 완화 및 통합 지원, 21세기 미국-아프리카 파트너십 구축, 평화로운 북극 유지, 바다·대기·우주 보호

1-2. CISA 전략계획 2023~2025 (CISA Strategic Plan 2023~2025, `22. 9.)

| CISA는 2018년 설립 이래 최초로 향후 3년간 기관의 미션과 국가 사이버보안의 수준 강화의 이정표 역할을 할 전략을 발표

• **국가 사이버방어기관**(National cyber defense agency)이자 주요 기반시설의 보안을 위한 국가 조정자(National coordinator)의 역할 수행을 명시

• 사이버보안 뿐만 아니라, **미국 주요 기반시설 보호의 중심 기관**으로서 별도 조직을 통해 **테러, 표적화 공격, 자연재해 등 물리적 위협에 대한 대응 역량 강화**를 강조

- 지역사무소 운영 통합, 정보 공유 강화 등 **CISA의 주요 보호대상인 주요 기반시설 및 주·연방 정부와의 협력** 강조
- **(비전)** 미국 국민을 위한 안전하고 복원력 있는 기반시설
- **(미션)** 사이버·물리 기반시설에 대한 위험을 이해하고, 관리하며, 감소시키는 국가적 노력을 선도
- CISA 전략 계획은 **CISA가 통합기관으로서 임무를 달성**할 수 있도록 **4가지 목표를 정의**하고 **각 목표에 따른 과제**를 제시

[표 3] CISA 전략계획 2023~2025 4가지 목표 및 각 목표에 따른 과제

목표	과제
1. 사이버 방어	(1-1) 사이버 공격 및 사고를 대처하기 위한 연방 시스템 능력 강화
	(1-2) 미국 주요 인프라·네트워크 타겟의 사이버위협에 대한 CISA의 능동적 탐지 능력 향상
	(1-3) 치명적인 사이버 취약점의 공개 및 완화 추진
	(1-4) 사이버공간 생태계 개선을 통해 보안내재화 추진
2. 위험 감소 및 복원력	(2-1) 기반시설, 시스템, 네트워크에 대한 가시성 확대
	(2-2) CISA의 위험 분석 기능 및 방법론 개선
	(2-3) CISA의 보안·위험 완화에 대한 지침 개선 및 영향력 강화
	(2-4) 기반시설 및 네트워크의 보안·복원력 측면에서의 이해관계자 역량 강화
	(2-5) CISA의 위협 및 사고에 대한 대응 능력 향상
	(2-6) 선거 인프라의 위험 관리 활동 지원
3. 운영 협력	(3-1) 이해관계자 참여 및 파트너십 활동의 계획·이행 최적화
	(3-2) CISA의 운영 조직에 지역 사무소 완전 통합
	(3-3) CISA 프로그램·제품·서비스에 대한 이해관계자의 접근 및 사용 간소화
	(3-4) CISA 파트너십 기반과의 정보 공유 강화
	(3-5) CISA의 제품 개발 및 임무 수행을 알리기 위한 이해관계자 통찰력의 통합 강화
4. 기관 통합	(4-1) CISA의 거버넌스, 경영, 우선순위 강화 및 통합
	(4-2) 모든 부서가 상호 지원이 가능하도록 비즈니스 운영 최적화
	(4-3) CISA의 우수 인력 양성
	(4-4) 우수한 CISA 조직문화 발전

목표 1. 사이버 방어(Cyber Defense)

• 사이버 공간의 방어 및 복원력 확보를 위해 국가적 노력 선도

☞ CISA는 **주요 기반시설, 연방 및 주·지방(SLTT)정부, 민간 기반시설 및 미국 국민을 대상**으로 하는 **사이버위협을 방어**하기 위해 정부 차원에서의 조정 실시

☞ **주요 기반시설의 시스템과 네트워크**, 그리고 **기반시설이 제공하는 민관핵심기능**(NCF)*에 대한 **침투, 악용, 교란, 파괴 시도를 최소화**하는데 집중

* 민관핵심기능(National Critical Function) : 국가의 보안, 경제 안보, 공중 보건 및 안전 등에 영향을 줄 수 있는 국가의 주요 기능 요소

☞ **중요 취약점의 공개·완화 추진** 및 넓은 영역에서의 **사이버 생태계의 보안 강화**

– 사이버 생태계의 인력 부족 문제도 반드시 해결 필요

☞ 안전하고 복원력 있는 사이버 생태계 달성을 위해 공공·민간 부문의 협력 중요

• (과제 1-1) 사이버 공격 및 사고를 대처하기 위한 연방 시스템 능력 강화

– CISA는 국가 사이버 방어 태세 개선을 위해, 연방 기관의 변화를 돕는데 전념하고 있으며 이를 위해 다양한 수행 방법 추진 필요

※ 현대적·탄력적인 기술 채택 촉진, 사고 대응 능력 향상, 연방정부에 대한 공급망 위협 억제, 연방 네트워크 전반의 사이버위협에 대한 가시성 강화 등

– 연방 민간 기관 중에 강력한 사이버보안 절차를 채택 및 평가하고, 혁신 서비스 및 역량 제공을 통해 기관의 효과적인 보안 프로그램 구축 지원

• (과제 1-2) 주요 인프라·네트워크 타겟의 사이버위협에 대한 CISA의 능동적 탐지 능력 향상

– 국가의 시스템과 정보에 지속적으로 접근하려는 적의 위협에 직면해 있으며, 이에 대한 탐지·예방 능력은 운영 가시성 확장에 달려 있음

– CISA는 산업계 파트너 협력을 통해 연방 및 주·지방 네트워크 전반에 대한 능동적인 탐지 능력 향상

• (과제 1-3) 치명적인 사이버 취약점의 공개 및 완화 추진

– CISA는 공공·민간 기관 및 사이버보안 연구단체와 협력하여, 알려지지 않은 취약점의 식별 및 보고를 장려하고 완화를 추진

– 주어진 권한 및 역량을 활용하여 완화되지 않은 취약점 식별 및 선제적 조치를 취하고, 사이버안전검토위원회 및 기타 자문기관의 권고안을 시행

• (과제 1-4) 사이버공간 생태계 개선을 통해 보안 내재화(Security-By-Default) 추진

– CISA는 보안내재화를 위해 네트워크 방어 및 사이버 운영 관련최신 도구, 서비스, 역량을 개발 및 채택하고 기술 지원을 제공

– 안전한 사이버 생태계는 기술만큼 사람에 관한 것임을 인식하고, 중요 기술 부족의 해소를 위해 사이버 인력에 대한 국가적 노력을 지원

목표 2. 위험 감소 및 복원력(Risk Reduction and Resilience)

• 미국 주요 <u>기반시설의 위험 감소</u> 및 <u>복원력 강화</u>

☞ CISA는 **주요 기반시설 보호를 위해 국가 차원의 노력** 조율

☞ CISA는 <u>**미국 주요 기반시설 보호의 중심 기관**</u>이며, 16개 주요 기반시설 부문 중 **8개 부문의 SRMA*의 업무를 전담**하며, **다른 부문에 대한 SRMA들의 업무를 지원**

* Sector Risk Management Agency : 대통령정책지침/PPD-21에 의거, 미국의 주요 기반시설을 16개로 구분 및 각 부문에 대한 위험 관리 기관(SRMA) 지정

☞ 민관핵심기능(NCF)을 활용하여 위험 식별·분석 및 위험 감소를 위한 노력 집중

☞ 중대한 사이버 사고 및 대형 재해 발생 시, **즉시 사고 관리 및 복구를 지원**

• (과제 2-1) 기반시설, 시스템, 네트워크에 대한 가시성 확대

- 정확한 데이터 및 통찰 정보의 수집을 기반으로, 국가 주요 기반시설의 자산과 시스템에 대한 통찰력 강화 및 주요 기반시설 데이터 저장소의 역할 수행
- 혁신적인 도구 개발 및 파트너십 강화를 통해, 위협 및 취약점에 대한 가시성을 확보하고 잠재적인 위협 요소를 사전에 방지

※ 주요 기반시설 사이버 사고 보고법(CIRCIA, 2022)이 의회에 통과하여, 사이버 사고에 대한 정부의 가시성 개선을 추진 중

• (과제 2-2) CISA의 위험 분석 기능 및 방법론 개선

- CISA의 위험분석 능력과 방법론을 발전시켜, 국가 및 기반시설 부문에 전반적인 피해를 줄 수 있는 위험 파악 필요
- (과제 2-1)을 통한 가시성과 주요 기반시설 정보 및 식별 노력을 분석 방법론에 통합하여, 의사결정을 가이드할 수 있는 통합 분석 결과물 산출

• (과제 2-3) CISA의 보안·위험완화에 대한 지침 개선 및 영향력 강화

- 위험 감소 효과의 개선·확대를 위해, 이해관계자에게 적용가능한 전문기술 및 완화 방안을 제공하고 긴급 통신 시스템 강화
- 또한, 파악된 위험 우선순위와 이해관계자에게 가장 중요한 위험에 초점을 맞춘 IT 네트워크 위험 관리에 효과적인 지침 발표
- 화학시설테러방지표준(CFATS) 및 기타 법령에 의거, 고위험 화학시설의 보안 확보

• (과제 2-4) 기반시설 및 네트워크의 보안·복원력 측면에서의 이해관계자 역량 강화

- SRMA 등 여러 이해관계자들의 증가하는 요청사항 충족을 위해, CISA의 핵심 프로그램 및 위험 관련 권고사항을 적절히 확대
- 또한 내부 위협, 총기 사고, 폭발물 등 물리 보안에 대한 서비스 제공

• (과제 2-5) CISA의 위협 및 사고에 대한 대응 능력 향상

- CISA의 8개 부문 SRMA 역할 수행과 다른 부문에 대한 SRMA 지원을 위하여, 테러 공격, 표적화 공격, 자연재해 등 물리적 위협 및 사고 대응을 위한 CISA의 역량 강화 필요
- 사이버 사고 발생 시 운영중단을 최소화하고 신속한 복구 지원을 위해, 공공 및 민간에 사고 대응역량을 배치하는 등의 지원 역량 확보
- 국가대응프레임워크에 의거하여, 자연재해 등 국가·지역적으로 중요한 사건에 대해 대응기관 지원 및 자산·역량을 배치할 수 있는 태세 완비

• (과제 2-6) 선거 인프라의 위험 관리 활동 지원

- CISA는 선거 인프라 하위부문의 SRMA로서, 선거 인프라에 대한 위험 파악·특성화를 위한 연방 정부의 허브 역할 수행
- 선거 인프라 위험관리 기능 연계, 특화된 신제품 개발, 지방 공무원의 잘못된 정보 또는 허위 정보 관련 지원

목표 3. 운영 협력(Operational Collaboration)

• 국가 전체의 **운영 협력** 및 **정보 공유** 강화

☞ **정부와 민간 부문의 파트너십**은 국가 주요 기반시설 보호를 위한 총체적 노력의 기반
☞ CISA는 파트너십을 통해 **공동 책무 확대·강화**, 기반시설 보안 및 복원력 확보를 위한 **제품·서비스 제공, 지역 및 국가 차원의 정보 공유·협력 강화** 추진
☞ 지역 및 국가 차원의 적극적인 참여 및 협력이 필요하며, 주요 기반시설 보호를 약속할 수 있는 인정받을 수 있는 **CISA 브랜드 구축 필요**

• (과제 3-1) 이해관계자 참여 및 파트너십 활동의 계획·이행 최적화

- 기관, SRMA 등 넓은 범위의 이해관계자 영역 내에서, 이해관계자 참여를 계획, 조정 및 우선순위 지정
- 자신 있게 서비스를 제공하는 CISA 브랜드를 구축하고, 국가·지역 차원의 지원 캠페인 개발 및 지역·주제·기반부문별 협력 우선순위 조정
- CISA는 주요 기반시설 보안 및 복원력 확보를 위한 SRMA 및 국가 조정기관으로서, 협력을 위한 입법 및 정책의무를 이행

• (과제 3-2) CISA의 운영 조직에 지역 사무소 완전 통합

- 본사와 지역간 협업을 위한 프로세스 수립 및 운영관리 상호 지원
- 부문·정부 조정 협의회(SCC, GCC)와 같은 요소를 직접적으로 확대하여, 국가 차원의 파트너십 관리 프레임워크와 지역 간 연계를 강화

• (과제 3-3) CISA 프로그램·제품·서비스에 대한 이해관계자의 접근 및 사용 간소화

- 이해관계자의 요구와 상황에 따라 맞춤형 서비스를 제공하고, 이해관계자 그룹 확대 및 공정한 접근 노력

• (과제 3-4) CISA 파트너십 기반과의 정보 공유 강화

- 사고 시 적시 보고, 위협·취약점 공유 등 외부 파트너와 다방향 소통 강화 필요
- 정보공유 촉진을 위해 공동사이버방어협력*(JCDC) 등 새로운 협력체를 지속적으로 구축하고 기존 조직의 성숙 노력 필요

  * 민간 부문과 연방 사이버 생태계 통합을 통해 국가 사이버 위험도를 낮추기 위해 설립

• (과제 3-5) CISA의 제품 개발 및 임무 수행을 알리기 위한 이해관계자 통찰력의 통합 강화

- 외부 이해관계자는 피드백, 평가 데이터 등 다양한 방법으로 통찰력을 제공
- 이해관계자들의 통찰력·정보·데이터의 통합을 강화하여, 우선과제 및 의사결정, 맞춤형 개발 및 개선에 활용

목표 4. 기관 통합(Agency Unfication)

• **기능, 역량, 인력**을 하나의 CISA로 통합

☞ 기존 운영 간소화, 새롭고 유연한 기술 채택 등을 통해 **하나된 CISA로의 통합** 필요
☞ 조직적 사일로 문제* 해결, 서비스 향상, 이해관계자 만족도 상승 등을 위해 거버넌스, 경영, 우선순위 강화
* 사일로 문제 : 조직 내 부서간 장벽 혹은 부서 이기주의
☞ CISA의 가장 소중한 자산은 **인적 자원**이며, **올바른 조직문화 형성** 노력 필요
☞ 현재의 인력 양성에 집중하고 있지만, 미래 사이버 인력 구축도 중요함을 인식

• (과제 4-1) CISA의 거버넌스, 경영, 우선순위 강화 및 통합

- 사일로 문제 해결을 위해 부서간교환 프로그램을 시행하고, 우선순위 결정을 위한 거버넌스·경영 구조 수립
- 기획, 프로그래밍, 예산편성, 집행 및 평가(PPBEE) 프로세스를 거버넌스 체계 및 의사결정에 통합하여, 필수 기능(급여, 대금청구 등)의 효율적인 내부 관리 및 현명한 투자 결정 추진

• (과제 4-2) 모든 부서가 상호 지원이 가능하도록 비즈니스 운영 최적화

- 필요에 따른 기존 운영 간소화 및 현대적이고 안전한 서비스를 제공할 수 있게 하는 민첩·유연한 신기술 채택
- 리더 의사결정, 프로세스·협력 개선, CISA 전반에 걸친 정보·데이터 공유를 위해 시스템 및 데이터 통합 추진

• (과제 4-3) CISA의 우수 인력 양성

- 글로벌 인재 생태계를 구축하고, 새로운 영역에서 예비 인재를 찾고, 모든 직원 및 리더에게 교육 기회를 균등하게 제공
- 투명성 및 운영 효율을 높여 성과 높은 팀이 성장할 수 있는 환경을 조성하고, 고용승진 기회 개발을 통해 직원들에게 공정한 결과를 부여

• (과제 4-4) 우수한 CISA 조직문화 발전

- 공정하고 정의로운 조직 문화를 위해, 리더들이 보상·성과, 소통 및 직원 대우에 관한 투명성·공정성 장려 촉진

참고1 바이든 대통령 행정명령(EO), 정책지침(PPD), 메모(NSM) 현황('21~22)

[표 4] 바이든 정부, 관련 주요 정책 및 내용

구분	주요 정책	주요 내용
연방기관 네트워크 보안 강화	EO-14028 (2021.5)	(국가 사이버안보 향상) - 정부기관-민간(IT서비스 제공자) 간의 위협정보 공유 장벽 제거 - 연방정부 사이버안보 현대화 및 구현 - SW 공급망 보안 강화 - 사이버안전검토위원회(Cyber Safety Review Board) 설립 - 사이버보안 사고·취약점 대응에 관한 연방정부 Playbook 작성 - 이벤트 침입 탐지 이후 연방정부의 조사 및 완화 역량 강화 - 국가안보시스템 (DoD, EO에 규정한 사이버보안 방안 의무 수행)
주요 기반시설 보안	American Jobs Plan (2021.5)	(통신, 전력 등 사이버보안 활동을 준수하는 민간 부문을 대상으로 보조금 지급) - 개인정보보호, IT/OT NW에서의 악의적인 사이버활동 탐지·차단하는 기술 설치, 신뢰할 수 있는 외부공급업체 이용 등 사이버보안을 준수하는 통신업체, 정전 위험이 높은 지역, CI 등에서의 마이크로 그리드 및 분산 에너지 기반시설을 대상으로 보조금 지급
	NSM Cybersecurity for CI Control Systems (2021.7)	(주요기반시설 제어시스템 사이버보안 향상) - 'ICS Cybersecurity Initiative' 분야를 전력 뿐만 아니라 천연가스 파이프라인, 상·하수, 화학 분야까지 확대 - 분야 공통에 적용 가능한 CI 사이버보안 성과목표 개발 → (2022.10.27.) CISA는 NIST CSF을 보완하는 전 CI 분야에 공통으로 적용 가능한 사이버보안 성과목표 발표
기타 (사이버 방위)	NSM Improve the Cybersecurity of National Security, DoD and Intelligence Community Systems (2022.01)	(국가안보 및 DoD, 정보기관(ODNI·NSA, CIA 등) 시스템의 사이버보안 개선) - 국가안보시스템은 EO-14028에 명시된 사이버보안 요구사항과 동일하거나 그 이상의 보호조치를 적용 (다단계 인증, 암호화, 클라우드 기술, EDR 포함) - 사이버보안 사고의 가시성 향상 및 국가안보시스템에서 발생한 이벤트는 NSA(Classified system의 국가 관리자(National manager)에 보고 - 각 기관은 사이버위협으로부터 소관 국가안보시스템을 보호하고, 완화하기 위한 조치를 취하여야 함 → NSA에 알려지거나 의심되는 사이버보안 위협 및 취약점에 대해 특정 조치를 취하도록 요구하는 운영지침의 작성 권한 부여 & 해당 운영지침은 DHS와 공유 - 각 기관은 Classified 및 Unclassified 시스템 간의 데이터를 전송하는 도구인 'Cross-Domain' 솔루션을 보호해야 함 → 공격자를 이 도구를 활용하여 Classified NW에 접근할 수 있기 때문에 각 기관은 이러한 솔루션의 자산목록을 목록화 → NSA는 각 기관에 보안표준 및 테스트 요구사항을 수립하도록 지시

※ 미국은 긴 시간이 필요한 포괄적인 정책, 법률 제정 보다는 사이버위협에 즉각 대응 하기 위해 주로 대통령 공표 [행정명령 EO(Executive Order), 정책 지침(PPD, Presidential Policy Directive), 메모(NSM, Presidential Memorandum, National Security Memorandum)]을 통한 긴급 사안 처리

참고2 EO-14028 4절 소프트웨어 공급망 보안의 강화 세부내용

❖ EO-14028 4절 소프트웨어 공급망 보안의 강화 세부내용

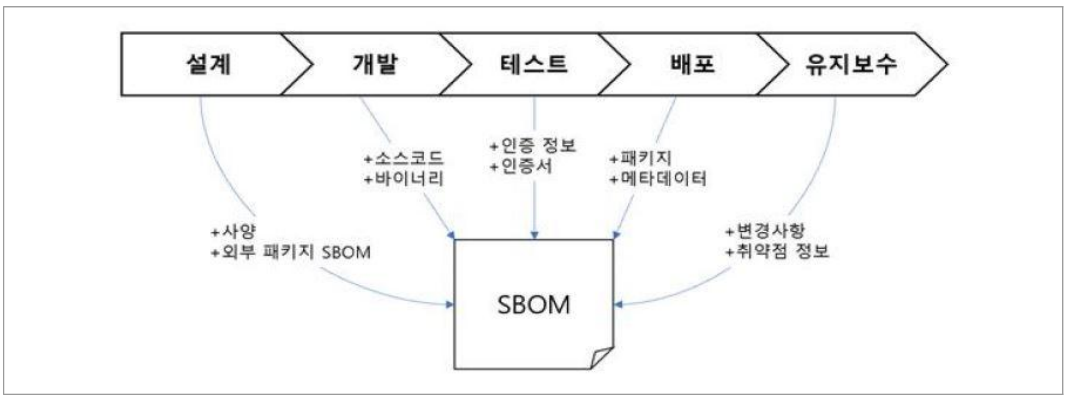
- ‘중요한 소프트웨어(critical software)’ 관련 보안 조치
  - 소프트웨어의 공급망 보안을 단계적으로 강화하기 위하여 ‘일반 소프트웨어’와 ‘중요한 소프트웨어’를 구분하고 ‘중요한 소프트웨어’에 대한 보안 조치 사항을 제시

    ※ ‘중요한 소프트웨어’를 인증되지 않은 접근 및 사용으로부터 보호, ‘중요한 소프트웨어’에서 사용되는 데이터의 CIA 보호 등

- SBOM(Software Bill of Materials)
  - SBOM의 최소 요소를 공표하고 SBOM*이 어떤 정보를 담아야 하는지, 어떻게 자동 생성해야 하는지, 그리고 생성된 SBOM을 어떻게 관리·운영해야하는 제시

    ※ ‘SBOM’ 이란? 소프트웨어를 빌드하기 위해 사용된 여러 컴포넌트에 대한 내용과 공급망 관계를 형식에 맞춰 기록하는 것을 말함

[그림 1] SBOM 개요



- 소프트웨어 테스트
  - 소프트웨어 검증에 권장되는 최소 기준을 마련하여 소프트웨어 생산자가 자체적인 검증 프로세스를 만들 수 있도록 지원

    ※ 테스트 종류 : 위협 모델링, 자동화 검사, 정적 분석, 동적 분석, 구성요소 검사, 버그 수정 등

- 가이드라인 및 지침
  - 안전한 소프트웨어 개발 환경, 코드의 완전성을 확보하기 위한 자동화 도구 도입, SBOM 제공, 안전한 소프트웨어 개발 방법에 대한 적합성 증명 등 공급망 보안 강화 방안 수록

1-3. EU, 사이버방어정책 (EU Policy on Cyber Defence, '22. 11.)

| '22년 11월, EU 집행위는 사이버위협에 대응하기 위한 EU의 사이버방어정책을 발표

- 우크라이나-러시아 전쟁으로 보다 **유럽 회원국의 강력한 방어 능력 구축 및 사이버 위기 대응 능력 강화**하는 **민군 협력의 필요성**을 제기
- 전력·에너지망, 네트워크, 운송 인프라 등 사이버공간에서 **민간과 군사 차원의 경계가 흐려지고 디지털 의존성 증가**함에 따라 대응 방안 마련

| 1. 강력한 사이버 방어를 위한 공동 대응 체계 마련

- 국방 관련 **주체 간 상황 인식 및 조정** 강화
  - 군사적 관점에서 EU 사이버 방어 조정센터(EUCDCC) 설립을 통한 국방 커뮤니티내 상황 인지 공유 체계를 제안, EU 내 공공보안 책임자간 유기적 체계 구축
  - 사이버 및 정보 도메인 조정센터(CIDCC) 프로젝트를 통해 사이버 공간, 전자기 환경 및 각종 인지 영역에 대한 전체론적 분석을 제공할 수 있는 대응력 구비
  - EU 정보분석센터(EU INTCEN)와 EU 군 참모 정보를 통합할 수 있는 단일 정보 분석 역량 프레임워크 구축 제안
  - 유럽방위청이 지원하는 군침해대응센터 네트워크(MICNET)에 모든 회원국이 참여하여 2023년부터 실제 운영 예정
- **민간 단체와의 공조** 강화
  - 군침해대응센터 네트워크(MICNET)은 사이버 방어 커뮤니티와 외부 이해관계자 간 다양한 정보 공유 및 플랫폼 역할을 수행할 수 있도록 유도
  - 개별 회원국이 운영중인 CSIRT(Computer Security Incident Response Teams)와의 공조 추진
  - EU 사이버위기 관리 조직과 민간의 연계를 향상시켜 민간의 사이버위기 상황 인지 능력 향상

| 2. EU 국방 생태계 확보

- 방어 생태계의 **사이버 복원력 강화**
  - 사이버 복원력 강화를 위해 회원국의 군사 인프라와 공동방어 임무, 주요 기반시설, 방위 산업, 연구기관을 대상으로 한 보안 조치와 투자 촉진
  - 최근 발표된 사이버 레질리언스 법(Cyber Resilience Act)을 통해 제품의 보안 요구사항 마련 의무를 부과하여 제품 전반의 보안성 향상
  - 기존 EU 회원국 사이버보안 인증에 대한 통합 체계를 마련하여 방위산업에 진입하기를 희망하는 기업들의 의욕을 고취

- EU 사이버 방어 **상호 운용성과 표준 일관성** 보장
  - 유럽연합 차원의 공동 연구개발과 조달 이니셔티브를 염두한 차세대 사이버 방어 요구사항을 통한 공동 협력 추진
  - 유럽 방위청과 유럽군의 사이버 방어 상호 운용을 위한 권장 사항을 개발하여 테스트, 평가 및 인증을 통해 신속하고 신뢰성 높은 기술 개발 추진

3. 사이버 방어 역량 강화 투자

- 전방위적 첨단 **사이버 방어 역량 개발**
  - 사이버 방어 개발 프로젝트에 대한 회원국 참여 확대를 위해 기술 스펙트럼에 걸친 투자 확대 및 연구개발 실시
  - 민간 영역의 기술 발전이 빠르고 보안 제품 시장이 빠르게 성장하고 있어, 사이버 방어를 위한 자체 역량 개발 필수
- 민첩하고 경쟁력 있는 혁신적 유럽 **방어 산업 구축**
  - EU 첨단기술 방어 산업은 민간기업의 비중이 매우 높고, 주로 외부 시장에 의존하므로 군사용 솔루션에 특화된 요구사항 반영을 위해 해외 기술 의존성 감소 필요
  - 유럽방위기금을 통해 디지털 유럽 프로그램과 연계 사이버보안 기술 개발 독려
  - 양자, AI 등 신기술에 특화된 R&D 로드맵 개발을 통해 사이버 방어 및 산업의 교구를 수용할 수 있는 정책 개발
- EU 사이버 방어 **전문인력 확보**
  - EU의 사이버 관련 직무능력 부족의 심화에 따라 핵심 기반시설 방어와 첨단 기술 개발을 위한 인력 확보
  - EU의 교육 요구 사항 분석을 기반으로 회원국은 사이버 방어 분야의 교육 활동 및 연습을 추가로 개발하고 공통 커리큘럼의 생성, 모범사례 공유 등 실시
  - 각 회원국의 국방부와 군 조직이 민간 대비 경쟁력 있는 조건과 보상 체계를 마련할 것을 권고

4. 문제 해결을 위한 파트너십 강화

- **EU-NATO 파트너십** 강화
  - 유럽연합과 NATO의 전략적 파트너십을 안보의 필수 요소로 인식하고 사이버 방어 분야를 포함한 다양한 위협에 대한 공유 체계를 상호주의에 입각하여 강화
- 동맹국과의 **파트너십 강화** 및 사이버안보 **역량 구축 지원**
  - 안보·국방에 대한 긴밀한 파트너십 필요성 증가에 따라 정보공유 등 상호 이익을 추구할 수 있는 협력 발전
- **사이버 성숙도가 낮은 국가에 대한 역량 강화**
  - 파트너 국가의 사이버 복원력 및 국방협력 강화
  - EU 공동 외교 미 안보 정책에 부합하는 EU 후보 국가와도 긴밀한 협력

Ⅱ

영국·프랑스 사이버보안 전략

2-1. 영국, 국가사이버전략 2022 (National Cyber Strategy 2022, '21. 12.)

| 영국 정부는 2025년 달성을 목표로 하는 '국가사이버전략 2022'를 발표

- 본 전략의 이전인 첫 번째 전략('11~'16)과 두 번째('16~'21) 모두 제목이 '국가사이버보안전략'이나, 이번에는 **'보안'을 생략하여 더욱 포괄적 정책임을 표방**
- 특히, 사이버범죄에 대해 **경찰·국방력 강화, 법개정을 통한 첩보 등 공격적 수단을 적극 고려**했다는 점에서 이전 전략과 차별화

| 1. (사이버 생태계) 영국의 사이버 생태계 강화

- 사회 전반을 아우르는 접근으로 국내 기관간 협업 강화
  - 국가사이버자문위원회, UKC3(UK Cyber Cluster Collaboration) 등 지역·공공·산업·학계 협업 강화
- 기술역량 강화 및 다양성 증진
  - 사이버부대(National Cyber Force) 등의 사이버인력 다양화, 포스트학사 훈련프로그램, 학부생 CyberFirst 장학금 제도 등을 통해 사이버인력 고급화
- 성장 및 혁신의 육성
  - 기존 기업지원 사업 통합 Cyber Runway 신규 운영, NCSC(국가사이버안전센터) 첼트넘센터를 National Cyber Innovation Centre로 업그레이드하여 스타트업 및 해외진출 지원

2. (사이버 복원력) 복원력을 갖춘 발전적인 디지털 영국 구축

- 신흥기술에 대한 예측, 진단 및 실행
  - 모든 정부부처 대상 NCSC의 사이버진단체계(CAF) 적용 및 기반시설 대상 적용 확대, GCCC (Government Cyber Coordination Centre) 신규 설치를 통한 사고 및 취약점 관리 일원화
- 사이버공간을 위한 기술 육성 및 유지
  - 기관·산업계 위협관리 강화, 뱅킹·쇼핑·이동통신 분야 등 온라인서비스 악성콘텐츠 차단강화, 해외직접투자(FDI) 사전심사 강화, 공급망 다양화, 2030년까지 정부 핵심기능 대상 복원력 구축 등
- 대비, 대응 및 복구
  - '25년까지 기존 기능을 대체할 신고 및 분석체계 구축, 정부차원의 피해자 지원 및 기반시설 사이버훈련 지원 등

3. (기술적 우위) 사이버파워*에 필수적인 기술 선도

* 5G/6G, AI, 블록체인, 반도체/프로세서, 암호인증, IoT 등 기존 및 신흥기술

※ 2026~7년까지 R&D 예산으로 220억GBP(약 35조원) 투입예정 ('2016~21년 19억GBP(약 4조원))

- 사이버보안·복원력을 위한 사이버위협 이해
  - NCSC의 연구역량을 확장, 4개 연구기관 및 19개 대학연구소 지원, 미래이슈탐색(horizon-scanning) 기능을 구축하여 R&D 및 정책개발 지원
- 기관 및 국민을 위한 사이버공격 예방 및 격퇴
  - 정부의 디지털보안내재화, 양자컴퓨터 보안모델 설계사업 등을 영국 AI기업에 전수하여 글로벌 우위 확보, 텔레콤 장비 공급망 다양화
- 국가 암호화기술 기업 보호
  - 군·정보기관 등에서 사용하는 암호기술 투자 및 NATO제공, Five Eyes 등 동맹국과 국제표준 활동 선도 및 수출확대
- 커넥티드 기술 확보 및 보안위협 최소화
  - 커넥티드 제품의 최소보안기준 구축, 안전한 전기자동차 충전소 등 스마트 에너지 시스템 구현, 클라우드 등 디지털서비스 사업자 규제 강화
- 글로벌 기술 표준화 활동
  - ITU, UN IGF(Internet Governance Forum) 등 글로벌 포럼 적극 참여, G7 국가가 운영하는 디지털 표준 그룹내 정보공유 강화

| 4. (글로벌 리더십) 안전·발전적 국제질서를 위해 글로벌 리더십 및 영향력 증진

• 공동대응활동 및 상호 사이버 복원력 강화

- 동유럽·아프리카·인도태평양 대상 사이버 역량개발 지원 및 중동·미주 주요국과의 동맹 유지, 글로벌 공급망 보호에 집중
- 해외 주재 외교관을 통해 사이버방역 캠페인 활동 추진(데이터·IP 탈취 등), NATO 회원국과 함께 사이버 보안 역량 개발 지원

• 자유·개방·평화·안전한 사이버공간을 위한 글로벌 거버넌스 확립

- OSCE(유럽안보협력기구), ASEAN, GFCE(글로벌사이버전문역량포럼), UN과 협력하여 부다페스트 협약에 상응하는 새로운 국제조약 추진, ICANN 및 IGF 활동 강화

• 영국의 전략적 우위를 위해 사이버역량 활용 및 수출

- 사이버공간의 인권·다양성·성평등을 위해 국제 가치 기반 캠페인 추진, 중소기업 지원 강화, 사이버보안 대사 프로그램 등 G2G 추진

| 5. (위협 대응) 사이버공간 위협요소 탐지·차단·방지를 통해 국가안보 강화

• 위협정보의 탐지, 조사 및 공유

- 정부·경찰·민간영역 전문가 활용 사이버범죄자·국가 상시 조사
- 국립범죄청(NCA)의 사이버정보력 활용 법집행 기능 강화
- 앨런 튜링 연구소(영국 수학 컴퓨터 연구소)와 협력, AI 활용 사이버공격 탐지 연구 추진

• 사이버범죄자·국가 저지 및 차단

- Counter State Threats 법안개정을 통해 법집행력 강화(첩보활동 신규포함)
- 사이버범죄 근절 및 경찰력 강화를 위해 '범죄수익법2002*' 개정 추진

  * 자금세탁방지·조사권한 등 범죄 수익금 관련 법률(Proceeds of Crime Act 2002)

- 사이버부대(NCF), NCSC, 국립범죄청간 협업 극대화로 랜섬웨어 퇴치
- 경찰청장협의회(NPCC)를 통해 사이버전문가 육성, 신흥기술 악용 대응

• 국가안보 및 범죄예방을 위해 사이버공간 방어

- 장기적으로 사이버부대 규모 확대, 공격적 사이버작전 실시
- 암호화폐 관련 대응을 위해 경찰의 기술적 역량 개발
- 新 통합작전개념2025* 일환으로 사이버역량 통합, 사이버군사합동작전 추진(민·관·군)

  * Integrated Operations Concept 2025 (영국 국방부, 2021.8월)

2-2. 프랑스, 국가전략 2022 (Nationale Stratégique 2022, `22. 11.)

| 우크라이나-러시아 전쟁을 계기로 유럽 방위 및 전략적 자율성의 범위하에 전쟁에 대한 대비 태세 강화와 동맹을 강화하기 위한 노력 명시

• 군사적 억지력과 더불어 **사이버위협으로부터 강력한 복원력을 확보**하고 긴장관계에 있는 **글로벌 사이버안보 거버넌스의 주도권과 전략적 연대**를 명시

[표 5] 프랑스 국가전략 2022 10대 목표 및 세부 내용

목표	세부 내용
1. 강력하고 신뢰할 수 있는 핵 억지력	(1-1) 유럽차원의 프랑스의 핵 억지력과 행동의 자유 보장
	(1-2) 효과적이고 독립적이며 주권적인 억지력 유지
2. 단합되고 회복력 있는 프랑스	(2-1) 프랑스의 집단, 내부적 복원력 강화
	(2-2) 사회, 국가에서 지속 가능한 국방 사고방식 촉진
3. 국방 사고 방식에 기여하는 경제	(3-1) 군 관련 공급망 확보 및 생산 재고 확보
	(3-2) 전쟁경제를 준비하기 위한 생산 및 지원주기 감소
	(3-3) 위험관리를 고려한 규제, 규범, 조달 및 지원 간소화
4. 최고 수준의 사이버복원력 확보	**(4-1) 프랑스 전체의 사이버 복원력 향상**
	(4-2) 프랑스의 사이버안보 모델의 성과 통합·강화
	(4-3) 사이버 복원력 최고 수준에 도달하기 위한 장기적 투자 강화
5. 모범적인 동맹국으로서의 프랑스	(5-1) 유럽방어에서의 프랑스가 동맹의 핵심 역할을 확인
	(5-2) 동맹 내에서 프랑스의 고유 역할 강화
	(5-3) EU-NATO 협력 강화
6. 프랑스를 원동력을 유럽의 전략적 자율성 강화	(6-1) 유럽의 전략적 자율성을 둘러싼 협력 실시
	(6-2) 유럽 방위 산업 역량을 전면에 등장
	(6-3) 유럽인들의 행동력 강화
7. 신뢰할 수 있는 주권, 안보의 파트너 프랑스	(7-1) 고 부가가치를 제공하는 파트너
	(7-2) 군비경쟁, 대량 살상 무기의 확산 및 재래식 무기 확산 방지
8. 평가 및 의사결정의 자율성 보장	(8-1) 민첩한 지능 및 감시 능력 개발
	(8-2) 기술 역량 강화
9. 하이브리드 분야에서 방어 및 행동 능력	**(9-1) 하이브리드 공격에 대한 공격에 대응 및 통제**
	(9-2) 정보 조직간 싸움에서 사이버 공격에 대한 광범위한 대응
	(9-3) 우주 및 통신 인프라에 대한 악의적인 활동 감시
10. 다중 환경 및 분야에서 고강도 군사 작전 수행 능력	(10-1) 의사 결정의 자율성 강화
	(10-2) 글로벌 연합에 대한 기여
	(10-3) 프랑의 국민과 영토를 보호하기 위한 조치 강화

| 목표 4. 최고 수준의 사이버복원력 확보

- 프랑스 전체의 **사이버 복원력** 향상
  - 공공·민간부문의 노력을 통해 대규모 공격에 대비하고 디지털 플레이어들에 대한 역할에 대한 확실한 정의
- 프랑스 **사이버안보 모델의 성과 통합·강화**
  - 2008년부터 수립되고 정기적으로 강화되고 있는 프랑스 안보 모델의 성과를 EU 모범사례로서 인정받도록 하고 프랑스의 사이버안보 모델을 EU 지침에 가능한 빨리 반영되도록 노력
- **사이버 최고 수준에 도달**하기 위한 장기적 투자 강화
  - 모든 공공서비스의 사이버안보 수준 강화와 사이버안보 문제에 대해 모든 이해 관계자를 참여 조치
  - 디지털 세계의 모든 이해관계자는 사이버위협에 대해 교육받고, 위험과 관련된 교육을 통합, 공급망과 국가의 보안을 위해 노력

| 목표 9. 하이브리드 분야에서 방어 및 행동 능력

- 프랑스의 주요 전략적 경쟁국은 **직접 및 간접, 군사 및 비군사, 합법 및 불법, 그리고 종종 원인 규명하기 어려운 행동 수단의 의도적으로 모호**한 조합인 **하이브리드 전략을 사용**
  - 이러한 위협은 민주주의를 방해하고 도덕적 권위와 응집력을 약화시키거나, 경제·국방 잠재력을 감소시키는 것이 목표
- (조직개선) 하이브리드 공격에 대응하기 위해 위협을 식별 및 평가하고 적절한 보호 매커니즘을 가진 대응력이 뛰어난 통합 조직 구성
  - EU의 전략적 방향성과 NATO2030 개념에 따라 동맹국과 파트너의 적극적인 활용
- **(행동실행) 외국 경쟁국과 정보 조직의 사이버공격 등 프랑스에 대한 광범위한 공격에 대한 방어와 치외법권과 싸우기 위한 툴킷 채택**
  - 적대 세력이 중개자로서 범죄조직, 무장 단체 등을 활용하는 것에 대한 공동 대응
- (주요 인프라 보호 강화) 수중 및 우주 통신 인프라에 대한 악의적인 행동에 대한 감지, 평가, 억제 차단하는 수단을 개발하기 위한 노력

Ⅲ

독일·일본 사이버보안 전략

3-1. 독일, 사이버보안전략 2021(Cybersicherheitsstrategie fr Deutschland 2021, `21. 9.)

| 독일 정부는 “사이버보안전략 2021” 발표를 통해 향후 5년간 독일 사이버보안 정책의 기본적인 방향을 설정

- ’16년 이후 발생한 **사이버위협, 환경 변화에 대응하고 세부 전략 목표 및 조치를 추가·보완**
- 전략의 방향성을 제시하는 4개 지침과 함께, **4개 행동영역으로 구분된 44개의 세부전략**으로 구성
  - 총 세부전략 개수 ’16년 29개 → ’21년 44개로 증가 (신규 31개, 유지 13개)

[표 6] 사이버보안전략 4개지침

내용
1. 국가, 경제, 과학 및 사회의 공동 과제로 사이버보안 설정 - 사이버위협에 대한 공동의 해답을 찾기 위해 협력과 신뢰가 필요하며 국경을 넘어 유럽 및 국제 협력 네트워크 마련 필요
2. 국가, 경제, 과학 및 사회의 디지털 주권 강화 - 디지털주권을 “디지털세계에서 독립적으로 개인 및 기관의 역할을 수행할 수 있는 능력과 가능성”으로 정의하며 2021 사이버보안전략의 중심 지침이라고 강조
3. 안전한 디지털화 구축 - ’16년과 비교하여 전자정부법, 5G 네트워크에 대한 보안, 전자 신원증명 등이 강조되고 디지털화에 대한 요구와 기대가 높아짐에 따라 사이버보안은 디지털화 성공을 위한 기본 요구사항이 됨
4. 측정 가능하고 투명한 목표 설정 - 향후 체계적인 업데이트를 위해 측정 가능하고 투명한 목표가 설정되어야 하며 정기적인 점검이 필요, 전략목표별 지표를 개발하여 목표 달성 여부를 임기 말에 평가

행동영역 1. 디지털 환경에서 시민들의 자기결정권 보장

- 시민들이 디지털 기술의 기회를 활용할 수 있도록 하고, 스스로 위험성을 인식하고 평가하는 등 사이버보안 역량을 강화

※ '16년도 전략 기준, 3개 전략 유지 및 4개 전략 삭제

[표 7] 행동영역1 세부전략(10개)

내용
(1-1*) 정보 제공 및 지원을 통한 모든 사용자(시민, 중소기업, 정부 기관)의 디지털 역량 제고 - 사이버위협에 대한 공동의 답을 찾기 위해 협력과 신뢰가 필요하며 국경을 넘어 유럽 및 국제 협력 네트워크 필요
(1-2) 보안 솔루션의 사용자 친화성 향상
(1-3) 디지털 소비자 보호를 위한 정부의 제공 확대 - 공급자 연락처 제공, 소비자 상담 센터 협력 및 디지털 소비자 보호 자문위원회의 자문
(1-4) 사이버안보 제품 및 서비스에 대한 통일된 유럽 보안 요건 - 인증마크 부착, IT 보안 레이블 도입 등
(1-5*) 안전한 전자 신원 증명 - 절차에 대한 요구사항 정의 및 통일성 있고 포괄적인 솔루션 생성 등
(1-6) 사물인터넷(IoT), 인공지능(AI) 시스템 등을 고려한 더 넓은 의미에서 사람과 사물의 안전한 전자 신원 보장 및 알고리즘·데이터·문서의 신뢰성 무결성 보호
(1-7*) V2V(차량 간 통신), V2C(차량과 클라우드 통신) 등 안전한 통신 및 웹사이트를 위한 전제조건 생성 - 안전한 통신 프로토콜 운용을 위한 암호화 등 보안 조치 수행
(1-8) CVD(Coordinated Vulerability Disclosure) 보안 프로그램 촉진 - 보안 취약점 발견 시 즉시 연락→패치 및 업데이트 전 공개 커뮤니케이션 여부 고려→폐쇄 조치 결정 등 프레임워크 제공
(1-9) 자주적, 자결적 행동을 위한 전제조건으로 암호화 구현 - 암호화 기술 사용 촉진, 법적·경제적·기술적·장벽 제거 등
(1-10) AI를 통한 IT 보안과 AI를 위한 IT보안

* : '16년도 유지 전략

| 행동영역 2. 국가 및 기업의 사이버보안에 대한 공동 대응

• 경제 전반에 걸쳐 사이버보안을 강화하기 위해 정부와 기업의 긴밀한 협력(중소기업 중심), 주요 기반시설의 안전 확보

※ '16년도 전략 기준, 4개 전략 유지 및 2개 전략 삭제

[표 8] 행동영역2 세부전략(13개)

내용
(2-1) 사이버보안환경 조정에서 국가사이버보안위원회(NCSR)* 역할 강화 * 연방정부를 위한 사이버보안 자문 기관으로 정부부처 간 협력증진을 위한 범정부 플랫폼
(2-2) 사이버보안 분야에서 정부·기업·학계·시민사회 간 협력 강화
(2-3*) 사이버 공격에 대한 정보기반을 구축해 신뢰할 수 있는 정보교환 플랫폼 마련
(2-4*) 독일 내 기업 보호 - 이니셔티브 및 중소기업 보호를 위한 특별 자금 마련 (Go-digital, Digital now)
(2-5*) 독일 디지털경제 강화 - 모빌리티, 에너지 전환 산업, 스마트시티, 인더스트리 4.0, 건강, 금융 분야의 조치, 표준 권장 사항 마련
(2-6) 기업을 위한 통일된 유럽 규제 프레임워크 형성
(2-7) EU 단일시장을 위한 안전한 IT제품·서비스 및 시스템 연구 개발 촉진 - 5G, 6G 기술 개발 및 도입
(2-8) 보안설계(Security by Design) 접근 방식을 통한 미래 핵심기술 보안 강화 - 사용자를 보호하기 위해 핵심기술의 보안체계 구축을 개발 프로세스 중심요소로 고정
(2-9) 양자 기술을 통한 IT보안 확보
(2-10) 혁신 주기(Time-to-Market)와 테스트, 승인 절차 조화
(2-11*) 주요기반시설 보안 개선 - 핵심기반시설 운영 지원, 핵심기반시설 운영자의 자발적 국가 정보 교환, 사이버 공격 조기 식별 및 차단 가능성 등을 포함한 프레임워크 제시 등
(2-12) 사이버보안 인증 - 사이버보안 인증 프레임워크 구현 적극 지원 및 인증 체계 개발 추진
(2-13) 미래 통신 인프라 확보 - 5G, 6G 통신 네트워크 및 우주 기반 인프라의 보안, 특히 6G 표준화 형성 및 시장 출시 기반 마련 강조

* : '16년도 유지 전략

| 행동영역 3. 효율적이고 지속 가능한 국가 사이버보안 아키텍처

• 연방주 협력과 입법권한 강화 등을 통해 연방정부와 연방정보기술 보안청(BSI)*의 역할 확대

* 사이버방어센터, 국가CERT 등을 운영하고 민관협력을 주도하며 정부 컨설팅, 사이버위협 탐지·대응, 시민, 기업, 정부와 정보공유, 표준화 및 평가·인증 등을 수행

※ '16년도 전략 기준, 3개 전략 유지 및 8개 전략 삭제

[표 9] 행동영역3 세부전략(14개)

내용
(3-1) 사이버공격 예방을 위한 연방정부 능력 향상
(3-2) 연방정보기술보안청 기술적 운영부서*를 적합하게 네트워킹 * 국가 IT 상황 센터, CERT-Bund, MIRT(모바일사고대응팀) BSOC(EU의 국가연락사무소)
(3-3) 연방정보기술보안청(BSI)과 연방주 간 네트워크 확대를 통해, BSI를 연방형사경찰청(BKA), 연방헌법수호청(BfV)과 함께 독일 사이버보안체계 3대 중심축으로 발전
(3-4*) 국가사이버방어센터의 추가 발전 - 사이버위협에 대한 부서 간 정보 교환 및 조정 플랫폼으로의 발전
(3-5) 연방행정기관의 사이버 및 정보 보안 강화
(3-6) 선거 환경의 사이버보안 강화
(3-7*) 사이버공간에서 형사처벌 강화
(3-8) 제로데이 및 익스플로잇 공격 취약점에 대한 책임 있는 처리 촉진
(3-9) 암호화를 통한 보안성 확보, 암호화 없는 보안성 확보
(3-10) 사이버범죄 퇴치를 위한 연방형사경찰청 전문성 및 서비스 향상
(3-11) 보안영역 중앙정보기술기관(ZITIS)확장을 통한 보안당국의 디지털 주권 강화
(3-12) 예방, 교육, 탐지 등 사전 강화를 통한 사이버보안 수준 향상
(3-13*) 사이버보안의 방어 체계 강화 - 연방군의 네트워크 및 시스템 보호 체계 등
(3-14) 통신법, 텔레미디어법 등 전문 법률을 기술 발전에 맞게 조정

* : '16년도 유지 전략

| 행동영역 4. 유럽 및 국제 사이버보안 정책에서 독일의 적극적인 역할 유지

• 유럽 사이버보안 관련 전략 및 규정*의 독일 내 반영 및 추가 개발에 적극적으로 참여하고 국가간 협력 플랫폼 구축

* 디지털 10년을 위한 EU의 사이버보안전략, 네트워크 및 정보 시스템에 관한 지침 등

※ '16년도 전략 기준, 3개 전략 유지 및 2개 전략 삭제

[표 10] 행동영역4 세부전략(7개)

내용
(4-1*) 효과적인 유럽 사이버보안 정책 적극 수립
(4-2*) NATO의 사이버방위 정책 발전 지원
(4-3) 사이버공간에 대한 규범적 준거를 강화 및 책임 있는 국가 행동을 위해 노력
(4-4) 신뢰구축장치(confidence building measures) 지원
(4-5*) 사이버역량 구축을 위한 양자 간 지역별 지원 및 협력 강화
(4-6) 국제법 집행 강화 및 국제 사이버범죄 퇴치
(4-7) 효율적 범죄 대응을 위한 혁신적 솔루션 마련을 위해 EU와 협력

* : '16년도 유지 전략

참고3 독일 사이버보안전략 2016 주요 내용

❖ 독일 정부는 연방내무성이 제안한 “2016 사이버보안전략” 도입을 결정('16.11.9)

• 사이버공간에서의 기회를 최대한 이용하고 네트워크 정보인프라의 의미와 보호에 상응하는 수준의 사이버보안을 보장하기 위해 도입

[표 11] 독일 사이버보안전략 2016 4개 행동영역 및 세부전략

행동영역	세부전략
① 디지털 환경에서 시민들의 자기결정권 보장 (7전략)	– 이용자의 디지털 능력 향상 촉진 – 통신 및 웹서비스 안전 요건 구축 – 온라인 보안인식 제고 – 안전한 전자ID보장 – IT 보안에 대한 품질 인증 및 허용의 강화 방안 도입 – 디지털화에 대한 안전성 확보 – IT분야 보안연구 촉진
② 국가 및 기업의 사이버보안에 대한 공동 대응 (6전략)	– 주요기반시설의 안전 강화 – 사이버 공간에서의 독일 회사 보호 – 독일 IT 산업 강화 – 인터넷 서비스 제공자와의 협력 강화 – 민간 부문의 IT 보안전문가의 육성 – 신뢰할 수 있는 정보교환을 위한 플랫폼 구축
③ 효율적이고 지속 가능한 국가 사이버보안 체계 구축 (11전략)	– 국가사이버보안청의 확대 – 현장분석 및 대응 능력의 강화 – 사이버공간에서의 형사소추의 강화 – 사이버스파이와 사이버 사보타지에 대한 효과적 대응 – 외국에서 유입되는 사이버 공격에 대한 조기경보시스템 구축 – 내무성 산하에 정보기술센터(ZITiS) 설립 – 사이버보안 방어 체계 강화 – 독일 CERT 체계의 강화 – 연방행정기관의 IT 안전 확보를 위한 조치 – 연방 정부와 주 정부의 협력 강화 – 사이버보안을 위한 재원 확보 및 인적자원의 확보·육성
④ 유럽 및 국제 사이버보안정책에서 독일의 적극적 역할 유지 (5전략)	– 유럽 사이버보안정책의 적극적인 국내 반영 – NATO 사이버방위정책의 확대 개선 – 사이버보안 위협에 대한 국제적 대응의 적극적인 공조 – 협력 국가의 사이버 역량 강화를 위한 지원 – 국제적 형사소추의 강화

3-2. 일본, 新 사이버보안전략 2021 (サイバーセキュリティ戦略 2021, `21. 9.)

| 사이버보안기본법('14년 제정)에 근거한 3번째 발표된 중기 전략('21년~'23년)

- 사이버 공격의 **위협 주체로 중국, 러시아, 북한을 처음 구체적으로 명기**하고, **방위성 중심의 사이버 능력 향상을 강조**
- 'Cybersecurity for All'**을 정책목표**로 하고 다음의 3가지 방향성을 추구

1) 디지털 대전환과 사이버보안의 동시 추진

2) 사이버 공간전체에 대한 안전안심 확보

3) 사이버공격에 대한 안전확보 관점에서 동맹·우방국과의 협력 강화

| 1. 경제·사회·활성화 및 지속적인 발전

- 경영층의 보안의식 개혁
  - 디지털 경영을 위한 행동 지침 구현, 인센티브 제도 도입
  - 사이버보안 경영 가이드라인 제시
- 지역사회·중소기업의 DX(Digital Transfrmaion) with Cybersecurity
  - 지역 및 중소기업의 사이버공격을 사후 대응책 지원을 위한 사업 확대
- 새로운 가치 창출을 지원하는 공급망에 대한 신뢰성 확보
  - 공급망 및 데이터 유통 인프라를 정비하고, 보안 제품·서비스에 대한 써드파티 인증제도 확산 등을 추진
- 전국민 대상 디지털 소외 해소 및 디지털·보안 리터러시 향상
  - 디지털 활용지원 정보교육 등 다양한 대응책 마련

| 2. 국민이 안전하고 안심하며 살 수 있는 디지털 사회 실현

- 국민과 사회를 지키기 위한 사이버보안 환경 제공
  - (안전한 이용환경 구축) 공급망 관리 가이드라인 마련, IoT·5G 등 신기술 구현에 따른 안전 확보
  - (클라우드 서비스 보안) 정부기관·주요 인프라 사업자 등 대상 클라우드 이용 시 보안규칙 마련 및 ISMAP (정보시스템 보안관리 및 평가 프로그램)의 대응 등 보안성이 검증된 민간 클라우드 이용 촉진
  - (사이버범죄 대응) 사이버 범죄를 지원하는 악의적인 사업자를 적발하고 경찰의 사이버 사고 대응 체계 강화

- (포괄적 사이버방어) 사이버공격 대처에서 재발 방지 등의 정책 대응까지의 종합적 조정을 담당하는 국가 침해사고 대응(CERT) 기능의 강화

  ※ 취약점 대책, 기술 검증, 제어 시스템의 사고 원인 규명 기능 등 정비

- (사이버공간의 신뢰성 확보) 개인정보와 지적재산권 보유 주체에 대한 지원 및 정부조달, 주요기반시설, 국제 해저케이블 등의 IT 시스템·서비스의 신뢰성 확보

• 디지털청을 중심으로 한 디지털 개혁과 국가 사이버보안 정책 실행의 일원화

- 디지털청 주도로 국가 정보시스템 정비 방안에 사이버보안 기본 방침 마련
- ISMAP 제도를 운용하여 민간부문에서도 이용하도록 권고

• 경제사회 기반을 지원하는 각 주체별 역할 강화

- (정부기관) 정부기관 정보보안 대책 통일기준군에 근거한 보안 대책 추진과 감사·CSIRT 훈련·GSOC 등을 통한 정부기관 전반의 보안 수준의 향상
- (주요 인프라) '주요기반시설 정보보안대책 제4차 행동계획' 개정으로 보안 환경 변화 대응 역량 강화와 경영층 리더십 강조

  ※ 지방공공단체 정보시스템의 표준화 및 행정절차 등 온라인화를 위한 가이드라인 수정 등

- (대학·교육 연구기관) 첨단정보 보유 대학 등의 경우 위기관리 대응을 위한 연수 및 훈련, 공급망 위기 대책 등 강화 지원

• 다양한 주체 간 정보 공유·협력 및 대응경험 활용

- 분야·과제별 정보공유·협력 추진(ISAC을 포함한 정보공유강화)
- 포괄적 사이버방어를 위한 정보공유·협력체계 정비(국내외 유관기관과의 협력 강화)

• 대규모 사이버공격사태 등에 대한 대처능력 강화

- 평시 대규모 사이버 공격에 대응을 위한 태세 강화, 민관협력을 통한 보안인재 활용 등

3. 국제사회의 평화·안정 및 일본의 안전보장에 대한 기여

• 자유, 공정하며 안전한 사이버 공간 확보

- (사이버 공간의 법적 지배력 강화) 사이버보안에 관한 국제법적용에 대한 일본의 의견을 적극적으로 표명하고 동맹국의 지지를 얻어 국제법 적용강화를 추진
- (사이버공간의 규범 형성) 건전한 사이버 공간의 발전을 저해하는 국제규범의 변경을 위해 동맹국 및 민간단체 등과 협력강화

• 일본의 방어력·억제력·상황 파악능력의 강화

- (방어력) 방위성과 자위대의 사이버공격 대비 방어력 향상 및 첨단기술과 방위산업의 보안확보를 위한 민관연계, 정보공유 등

- (억제력*) 사이버공격 방해능력 강화와 외교적 수단·형사소추 등 대응 및 미·일 동맹 유지·강화

  * 억제력(deterrence by denial), 복원력과 함께 미국에서 쓰임

- (상황 파악력) 관계기관의 전국적인 네트워크, 사이버부대 및 인적 정보를 활용하여 사이버 공격 심층적 실태 확인 및 카운터 사이버인텔리전스(외국의 정보수집활동 방어) 추진

  ※ 비정부조직의 사이버공격에 대응하기 위해 부처간 및 국제협력 추진

• 국제협력·연계

- (정보 공유 및 정책 조정) 미국, 호주, 인도, ASEAN 등 우방국과의 부처 횡단 및 각 부처 단위별 중층적인 국제협력 틀 강화

- (국제 연계 강화) 국제 공동 사이버훈련 주도를 통한 국제 위상 강화, 개도국과의 산학관 연계와 ASEAN을 포함한 인도 태평양 지역 사이버보안 공동 대응 및 외교 강화

  ※ '2020.10월 '사이버보안 분야에서 개발도상국에 대한 역량 개발 지원과 관련된 기본방침'을 수립한 바 있음

- (타 국의 보안역량 향상 지원) 저개발 및 개도국을 대상으로 세계은행 등 국제기구 협력으로 사이버보안 능력 향상을 지원하며 국내 기업의 진출 기반 확보

| 4. 범부처·중단기 시책

• 연구개발 추진

- (산학관 생태계 구축) 과학적 이해를 심화하고 혁신 원천이 될 수 있는 연구 및 산학관 연계 진흥 시책 활용 촉진 및 연구자의 자유로운 연구 환경 조성

- (실천적 연구개발) 공급망 위기(5G 보안 등) 대응을 위한 기술검증체계 정비, 국내산업 육성·발전을 위한 지원책 추진, 사이버공격에 대한 파악·분석·공유 기반 강화, 암호 연구 등

- (중장기 기술 대응) AI-보안 기술(AI for Security, Security for AI) 연구 및 양자기술 등 기반 마련

• 인재확보·육성·활약 촉진

- (보안 인력양성 환경정비) 전문가나 최신 지식 등을 통해 사이버보안 비전담자도 관련 지식을 적극적으로 수용하기 위한 분위기 조성, 기업 및 조직 내 적재적소의 유동적 인재 이동 지원 체계 구축

- (교묘화·복잡화 위협 대응) 보안 자격제도 정비·개선 및 실천적 대응능력 향상을 위한 콘텐츠 개발 및 보안 인재 육성을 위한 공통기반 구축

- (정부기관 대응) 우수한 보안인력 채용을 위해 국가공무원시험에 디지털분야 합격자 적극 활용 및 부처별 보안인력 확충 및 매년 보안계획 갱신추진

• 전원(국민) 참가에 의한 협동, 보급진흥

- 사이버공간 보호를 위해 산학관의 포괄적 참여를 위한 실행 계획 구체화 및 개선

- 고령자 디지털 격차 해소 및 보안 강화 방안 검토

Ⅳ 시사점

4-1. 사이버보안에 대한 인식의 변화

| 선제적 대응을 위한 적극적 사이버 방어로 전환

- **전략 설계**시 수동적 방어에서 보다 **능동적으로 방어**하기 위한 **포괄적 접근 방식으로 전환**
  - **(미국, EU, 영국, 프랑스)** 사이버공격으로 인한 피해가 발생하기 전 또는 피해가 확대 되기 전에 **공격자의 의도를 미리 분석**하여 이에 대한 **조치를 사전에 수행**

| 핵심 기능의 지속적인 운영을 위한 사이버복원력 강화

- **알려지지 않은 사이버위협**이 발생하더라도 조직·시스템의 **중단을 최소화**하고 **핵심 기능이 신속하게 복구**되어 **지속적으로 운영**될 수 있도록 대비
  - **(미국, EU, 영국, 프랑스) 기존의 경계 중심의 보안이 아닌** 필요한 조직의 보안 최대 임계치를 미리 파악하여 **핵심 자산·자원에 대한 복구 체계** 마련

| 사이버보안의 중요성이 국가안보(안전, 경제, 사회 등) 차원으로 확대

- **사이버공간**에서 발생하는 악성행위가 **국가안보(공공안전, 경제발전)에 심각한 위협**임을 강조
  - **(미국, EU, 영국, 프랑스)** 우크라이나-러시아 **전쟁으로 촉발된 사이버戰, 주요 기반시설에 대한 테러** 등으로 **사이버보안 전략의 수립·개정, 거버넌스, 법·제도 개편**

4-2. 사이버보안 전략의 방향성

| 코로나19, 기반시설 위협 등으로 촉발된 사이버보안의 패러다임 전환

- **제로트러스트, 공급망 보안** 강화 등 디지털 환경 변화에 대응하기 위한 **신규 정책 및 기술 개발 강화**
  - **(미국)** 새로운 안보질서와 변화된 사이버보안 환경에 적시에 대응 할 수 있는 **사이버보안 정책 전환 체계 구축 및 R&D 강화**

| 주요 기반시설에 대한 보안 위험관리 의무 강화

- 전력, 에너지, 금융 등 **주요 기반시설**에 대한 **사이버보안 대비 의무를 부여**하고 보고·평가 사항 규정
  - **(미국, 독일)** 주요 **기반시설 위험평가(Risk assessment) 실시**, 사이버보안 감사, 위험관리 프로그램 등

| 협력체계의 중요성 강조 및 공동 훈련·방어 등 공조 강화

- 사이버보안 강화를 위해 **민간 및 국제협력·공조**를 통한 사이버보안 이슈의 적극적인 해결 강조
  - **(미국, EU, 영국, 프랑스, 독일, 일본)** 민관 사이버위협 **정보공유, 공동훈련, 글로벌 공조**를 통한 문제 해결, **공동 방어** 등

| 민간·공공 인프라에 대한 사이버사고 보고·조치 의무화

- **주요 인프라(민간포함)**에 해당되는 영역의 사이버 침해사고 발생시 **관계기관 보고 및 조치 등의 법적 의무사항을 부여**
  - **(미국) 공격 발생 이후 72시간內, 랜섬웨어 공격 대가 지급 후 24시간內 CISA에 보고 의무 부여**와 미준수 시 **벌금 또는 과징금 징수** 및 **민사소송 제기***

    * 주요기반시설 사이버사고 보고법(Cyber Incident Reporting for Critical Infrastructure Act of 2, '22. 3.)

KISA INSIGHT

DIGITAL & SECURITY POLICY

2023 VOL. 1

미국·EU·영국 등의 사이버보안 전략 분석 및 시사점

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY