ETRI Insight

기술정책 이슈 2022-03

사이버보안 분야 동향 및 이슈

기술전략연구센터
심진보·원용숙·홍아름·홍수지

정보보호연구본부
김익균·강유성·김건우·문대성·최병철 외

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

본 보고서는 ETRI 기술정책연구본부 주요사업인 “국가 지능화 기술정책 및 표준화 연구”를 통해 작성된 결과물입니다.
본 보고서는 ETRI 기술전략연구센터와 정보보호연구본부의 협업을 통해 작성되었습니다.

본 보고서의 내용은 연구자의 견해이며 ETRI의 공식 의견이 아님을 알려드립니다.

목 차

핵심 요약 1

Ⅰ. 사이버보안의 개념 및 중요성 7
1. 사이버보안 개념 및 범위 7
2. 사이버보안의 중요성 및 국가투자전략 연구의 필요성 10

Ⅱ. 사이버보안 정책 및 투자 동향 13
1. 주요국 사이버보안 정책 및 투자 동향 13
2. 국내 사이버보안 정책 동향 28
3. 국내 사이버보안 분야 정부 R&D 투자 현황 31

Ⅲ. 사이버보안 기술 동향 및 전망 42
1. 사이버보안 분야 중점기술 42
2. 국내·외 사이버보안 기술개발 동향 43
3. 사이버보안 기술의 진화 방향 51

Ⅳ. 사이버보안 시장 및 산업 동향 56
1. 글로벌 사이버보안 시장 전망 56
2. 주요국 사이버보안 시장 및 산업 동향 58

Ⅴ. 사이버보안 분야 R&D 이슈 63

참고문헌 67

표목차

[표 1-1] 정보보호 기술 분류체계 8
[표 2-1] 주요국 사이버보안 관련 정책 현황 13
[표 2-2] 주요국 중점분야 선정 현황 14
[표 2-3] 사이버보안 관련 주요국 정부 거버넌스 14
[표 2-4] 주요국 사이버보안 관련 법률 현황 15
[표 2-5] 주요국 민·관협력 강화 사례 15
[표 2-6] 미국 연방정부 사이버보안 예산 현황 18
[표 2-7] 일본 정부 사이버보안 예산 현황 22
[표 2-8] 정부 R&D 중 사이버보안 투자 현황 31
[표 2-9] 주요부처별 R&D 예산 중 사이버보안 투자 현황 32
[표 2-10] 개발단계별 정부 R&D 예산 중 사이버보안 투자 현황 33
[표 2-11] 수행주체별 정부 R&D 예산 중 사이버보안 투자 현황 34
[표 2-12] 지역별 정부 R&D 예산 중 사이버보안 투자 현황 35
[표 2-13] 정부 ICT R&D 예산 중 사이버보안 투자 현황 36
[표 2-14] 주요부처별 정부 ICT R&D 예산 중 사이버보안 투자 현황 37
[표 2-15] 개발단계별 정부 ICT R&D 예산 중 사이버보안 투자 현황 38
[표 2-16] 수행주체별 정부 ICT R&D 예산 중 사이버보안 투자 현황 39
[표 2-17] 지역별 정부 ICT R&D 예산 중 사이버보안 투자 현황 40
[표 2-18] ICT융합전문위원회 R&D 예산 중 사이버보안 분야 투자 현황 41
[표 3-1] 사이버보안 중점기술 및 세부 요소기술 42
[표 4-1] 글로벌 사이버보안 시장 전망 56
[표 4-2] 차세대보안 분야 중분류별 시장전망 57
[표 4-3] 2020년 글로벌 사이버보안 지수(GCI) 순위 58

그림목차

[그림 1-1] 사이버보안 기술 개념의 확장 9
[그림 1-2] 전세계 사이버보안 시장 규모 11
[그림 1-3] Gartner가 선정한 2022년 주요 기술 트랜드 12
[그림 2-1] 정부 R&D 중 사이버보안 투자 추이 31
[그림 2-2] 주요부처별 R&D 예산 중 사이버보안 투자 추이 32
[그림 2-3] 개발단계별 정부 R&D 예산 중 사이버보안 투자 추이 33
[그림 2-4] 수행주체별 정부 R&D 예산 중 사이버보안 투자 추이 34
[그림 2-5] 지역별 정부 R&D 예산 중 사이버보안 투자 추이 35
[그림 2-6] 정부 ICT R&D 예산 중 사이버보안 투자 추이 36
[그림 2-7] 주요부처별 정부 ICT R&D 예산 중 사이버보안 투자 추이 37
[그림 2-8] 개발단계별 정부 ICT R&D 예산 중 사이버보안 투자 추이 38
[그림 2-9] 수행주체별 정부 ICT R&D 예산 중 사이버보안 투자 추이 39
[그림 2-10] 지역별 정부 ICT R&D 예산 중 사이버보안 투자 추이 40
[그림 2-11] ICT융합전문위원회 R&D 예산 중 사이버보안 분야 투자 추이 41
[그림 5-1] 사이버보안 분야 STEEP 분석 결과 63
[그림 5-2] 거시환경 변화 분석에 기반한 사이버보안 분야 R&D 이슈 66

핵심 요약

사이버보안의 개념 및 중요성

- 기존에 사이버보안은 '정보보호'와 '정보보안'의 하위개념으로 분류되어 왔으나, ICT 기술의 발달로 사이버공간이 확장되고 사이버보안의 중요성이 커짐에 따라 현재는 '정보보호' 및 '정보보안'과 동일계위로 간주하는 추세

- 본 연구에서는 사이버보안에 관한 공통의미와 시장 및 현장성을 반영하여 사이버보안을 '정보보호', '정보보안'과 동일한 개념으로 간주하고, **"사이버공간에서의 위협으로부터 개인·기업·국가의 안전을 보호하는 정보보호 기술"로 정의**

- 사이버보안 국가투자전략 수립을 위한 기반 연구의 필요성
  - 최근 우리 정부는 변화하는 환경에 맞춰 ◁ 데이터 산업 활성화 전략('18), ◁ 국가 사이버안보전략('19) 등의 사이버보안 정책을 마련하고, 관련 R&D 예산을 확대하고 있으나 아직 체계적인 국가투자전략과의 연계는 부족한 상황
  - 사이버보안 분야에 대한 국가적 차원의 전략적 중요성이 커짐에 따라 **체계적·효율적인 국가투자전략 수립이 필요**하며, 따라서 **본 연구에서는 사이버보안 분야 국가투자전략 의사결정에 필요한 정책/투자현황/기술/시장/산업/이슈 분석**을 수행

국내·외 사이버보안 정책 및 투자동향

- 사이버위협의 범위와 영향력이 커지고 국가안보를 위협할 만큼 고도화됨에 따라, 주요국은 주요 국정과제로 운영하며 독자적 사이버보안 전략을 수립

- 데이터의 국가 간 이동 및 개인정보보호 등이 주요 이슈로 등장, 미국 중심의 서구 자유주의 국가와 중국을 비롯한 비자유주의 국가 간 입장 차 존재

- 미·중 기술패권전쟁이 사이버보안 영역으로 확장, 자국 중심의 글로벌 거버넌스 도모

- 국가 차원의 전략 수립과 함께 사이버보안 전담기관을 설치·운영하고, 전담조직의 권한을 강화하는 방향으로 발전 중

[주요국들의 사이버보안 분야 정책 동향]

국가		주요 정책	정책특징
미국		• 미국 국가 사이버 전략('18.9) • 국가 최상위 사이버보안 연구개발 전략계획('19.12) • 국가의 사이버보안 향상에 관한 행정명령('21.5)	사이버보안을 핵심 국정과제로 선정, 국가최상위 정책 수립하고 행정명령 발효
중국		• 국가 사이버공간안전전략('16.12) • 사이버안보 산업발전 3개년 행동계획안('21.7)	국가주도형으로 자국 이익 중심의 공격적 사이버보안 정책 전개
일본		• 사이버보안전략 2019-2021('19.9)	국가적 정책추진 방향을 반영하여, 3년 단위로 사이버보안전략 마련
유럽	EU	• 일반 개인정보 보호규정(GDPR) 및 NIS 지침 • 디지털 10년을 위한 EU의 사이버보안 전략('20.12)	데이터의 국가간 이동과 개인정보보호의 기반 마련
	영국	• 국가사이버보안전략 2016-2021('16)	주변국 파트너십과 국제협력 중요성 강조
	독일	• 독일을 위한 사이버보안전략 2016-2021('16)	국가안보 중심의 사이보보안정책 추진
한국		• 국가사이버안보전략('19) • 제 2차 정보보호산업 진흥계획('20) • 정보산업의 전략적 육성방안('22)	사이버보안의 핵심 지능정보기술 개발 확대 및 융합보안 강조

- 국내 전체 R&D 예산 중 사이버보안 분야 투자 동향 : 연도별 추이를 살펴보면, 사이버보안 분야의 정부 R&D 예산은 지속적으로 증가하고 있으나, **전체 정부 R&D 내에서 차지하는 투자 비중은 '19년 이후 하락**하는 추세

- 국내 주요부처별 정부 R&D 예산 중 사이버보안 포트폴리오 동향 : '20년 기준 과기정통부는 17.31조원으로(전체 90.9%) 가장 많은 예산을 지출, **과기정통부의 사이버보안 관련 예산과 비중 모두 증가**하고 있는 반면, 산업부는 예산과 비중 모두 지속적으로 하락하고 있으며, 중기부는 '19년 이후 예산과 비중 모두 하락 추세

- 개발단계별 국내 정부 R&D 예산 중 사이버보안 포트폴리오 동향 : '20년 기준 **응용연구 단계에서 가장 많은 비중(46.6%)**을 차지하고 있으며, 기초연구 단계가 가장 낮은 비중(8.7%)으로 나타남. 응용연구 단계는 예산은 증가하고 있으나 비중은 하락, 기초연구 단계는 예산과 비중 모두 하락 추세

사이버보안 기술동향 및 전망

- 미래 사이버 안전과 기술경쟁력 확보에 필수적인 중점기술 및 세부 요소기술들은 다음과 같이 분류 가능

[사이버보안 분야 중점기술 및 세부 요소기술]

중분류 기술	정 의	세부 요소기술
데이터 활용 보안	데이터 활용 전주기에 걸쳐 프라이버시 및 데이터 주권 보호 중심으로 데이터 활용성을 강화하기 위한 기술	• 고비도 암호 설계, 암호키 관리 및 검증기술 • 프라이버시 강화 컴퓨팅 기술 • 양자내성암호 분석 및 전환 기술 • 암호화 기반 데이터 검색/활용기술(동형암호 등) • 비식별화/익명화 기술, 데이터 주권강화기술
차세대 네트워크 보안	5G+ 융합서비스 및 미래 6G 네트워크 환경에서 보안위협을 대응하기 위한 지능형 사이버보안 기술	• 5G/5G+ 융합서비스 보안위협 대응 기술 • 사설 5G/특화망 네트워크 보안 기술 • 6G 네트워크 보안 내재화 기술 • 인공지능 기반 지능형 보안관제 기술 • 인공지능 기반 사이버공격 시뮬레이션 기술
시스템 · 디바이스 보안	대규모 IoT 디바이스를 포함한 다양한 ICT 기기의 안전한 사용을 위한 시스템·디바이스 보안 기술	• 시스템/디바이스 취약점 진단 자동화 • HW/SW 공급망 보안 기술 • AI기반 악성코드 분석 기술 • 지능형 IoT 디바이스 보안 기술
신 디지털 플랫폼 보안	Web 3.0, 메타버스 등 신 디지털 플랫폼 및 가상융합경제의 이용자 보호 기술	• 분산 디지털 신원관리 기술 • 메타버스 보안 기술 • 탈중앙화 가상경제 보안 기술 • 비대면 보안 기술
사이버 범죄 대응	다크웹, 랜섬웨어 등 사이버범죄 근원지 추적 및 디지털 포렌식 관련 기술	• 스마트기기 디지털 포렌식 기술 • 다크웹 사이버 범죄 근원지 추적 기술 • 랜섬웨어 공격 근원지 추적 및 피해복구 기술
융합 산업 보안	SoC 디지털 가속화에 따른 주요 기반 시설 및 국방 분야에 적용 가능한 IT와 OT의 융합보안 기술	• 국방 보안 기술(통신, 무기체계, 백신 등) • IT+OT 융합보안 기술 (해양·선박 등) • 저궤도 위성 통신 인프라 보안 기술
물리 환경 안전·보안	CCTV 등 영상보안시스템이 자율적으로 위협을 인식, 예측, 협업·대응하고 보안 역기능을 원천적으로 방지하는 개방형 영상보안 AI 기술	• 온-디바이스 초지능 CCTV 기술 • 개방형 영상보안플랫폼 기술 • 공공/민간 영상보안플랫폼 자율보호 기술

● 사이버보안 주요 분야별 기술 진화방향은 다음과 같이 전망됨

- **(데이터 활용 보안)** 데이터의 생산 주체인 개인의 권리를 최대한 보장하면서 자유로운 데이터 활용이 가능한 **개인데이터 신뢰·유통 기술 개발의 확산, 양자 컴퓨팅 대응 기술 개발 지속** 전망
- **(차세대 네트워크 보안)** 차세대 네트워크 보안에 성능향상을 위해 일부 활용되어 오던 **인공지능 기술이 보다 폭넓게 적용**될 것으로 전망되며, **5G/5G+ 융합서비스 보안위협 대응 기술의 중요성 증대**
- **(시스템·디바이스 보안)** 대량의 이기종 디바이스 간의 협업을 통한 **능동적인 보안**

위협 대응기술로 진화가 예상되며, **HW 기반 공급망 보안 기술이 강조**될 전망

- **(신 디지털 플랫폼 보안)** 모든 경제활동이 현실에서 가상세계까지 확대되는 메타버스 환경에서 사용자의 디지털 자산 및 프라이버시 보호를 위한 **새로운 패러다임의 보안 신기술 등장** 전망
- **(사이버 범죄 대응)** 사이버 안전망에 대한 요구가 증대되면서 범죄 억제력 강화를 위한 **범죄자 추적 및 사이버 복원력 기술이 확대**될 전망
- **(융합 산업 보안)** **SoC 디지털 가속화**에 따른 주요 기반시설 및 국방 분야에 적용 가능한 IT와 OT 융합보안이 활성화될 전망
- **(물리환경 안전·보안)** HW와 SW가 상호 종속되지 않는 안드로이드 기반 CCTV 플랫폼 활성화에 따라 **초지능을 보유한 CCTV 디바이스 확대** 전망

사이버보안 시장 및 산업동향

- 디지털 전환, 코로나19 등의 환경변화로 인해 사이버 위협이 증가하면서 글로벌 사이버보안 시장은 지속적으로 성장할 전망

[글로벌 사이버보안 시장 전망]

시장조사기관	전망
Mordor Intelligence (2021)	2021년 글로벌 사이버보안 시장은 약 1,329억 달러이며, 2022년부터 2027년까지 연평균 14.5% 성장할 것으로 전망
Grand View Research (2021)	2020년 글로벌 사이버보안 시장은 약 1,674억 달러이며, 2021년부터 2028년까지 연평균 10.9% 성장할 것으로 전망
Allied Market Research (2022)	2020년 글로벌 사이버보안 시장은 약 1,973억 달러이며, 2021년부터 2030년까지 연평균 9.5% 성장하여 4,786억 달러에 이를 것으로 전망
MarketsandMarkets (2021)	2021년 글로벌 사이버보안 시장은 약 2,179억 달러이며, 2021년부터 2026년까지 연평균 9.7% 성장하여 3,454억 달러에 이를 것으로 전망
Fortune Business Insights (2021)	2021년 글로벌 사이버보안 시장은 약 1,397억 달러이며, 2022년 1,558억 달러 2029년 3,763억 달러 연평균 13.4%
Research and Markets (2022)	2020년 글로벌 사이버보안 시장은 1,562억 달러이며, 2021년부터 2026년까지 연평균 14.5% 성장하여 3,522억 달러에 이를 것으로 전망

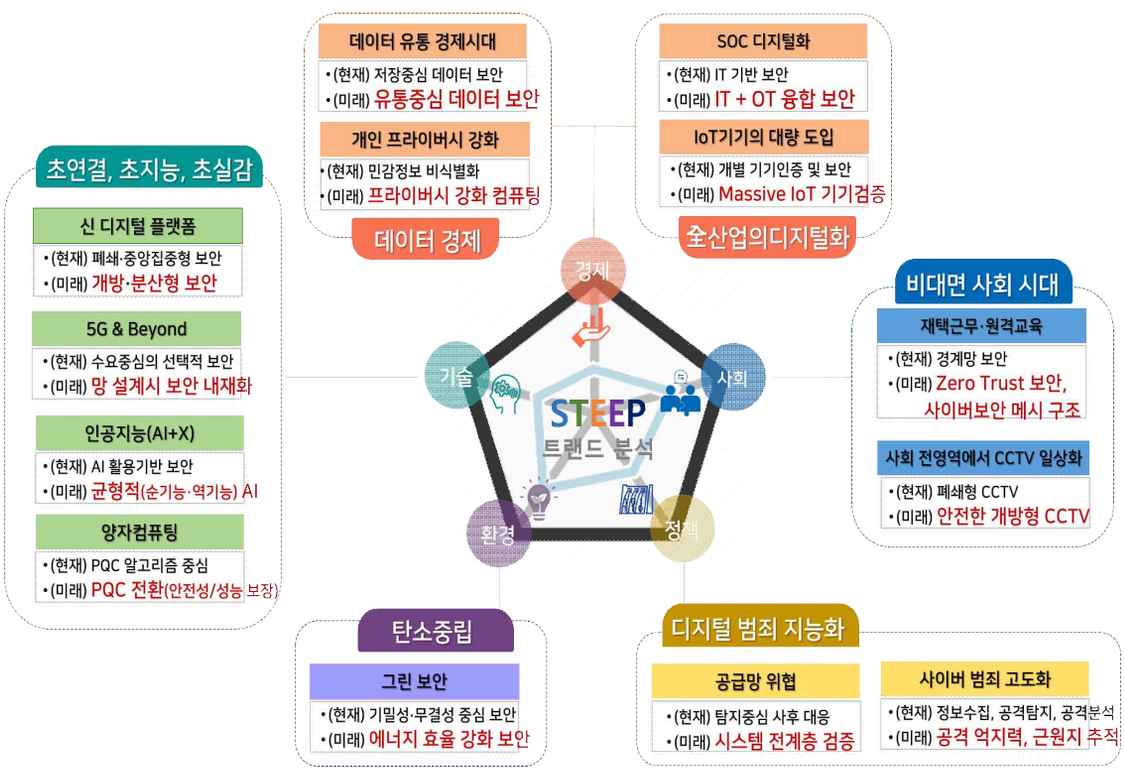
- 글로벌 사이버보안 시장에서 **정보보안 분야가 가장 비중이 높으며, 융합보안 분야는 현재는 비중이 낮으나 향후 급격히 성장**할 것으로 예측됨
- 벤처캐피털의 사이버보안 관련 스타트업에 대한 투자가 전세계적으로 급격히 증가

- 글로벌 주요국들의 사이버보안 산업 동향은 다음과 같음
  - **(미국)** 글로벌 사이버보안 시장은 미국이 주도하고 있으며, 미국은 시장 규모, 인프라 개발, 혁신, R&D 활동 등 전반적인 면에서 전세계에서 가장 앞서 있음
  - **(중국)** GDP 규모에 비해 글로벌 사이버보안 시장에서의 비중이 낮은 편이나, 향후 급격히 성장할 것으로 예상됨
  - **(영국)** 사이버보안 산업의 수준이 비교적 높으며, 기업 간 경쟁이 치열한 양상을 보임
  - **(일본)** 디지털전환으로 인해 사이버보안에 대한 필요성이 증가하고 있으나, 아직까지 사이버 보안 관련 의식이 저조
  - **(한국)** 기반 기술의 부족으로 응용제품 개발 위주의 중소 및 벤처기업 중심으로 발전

사이버보안 분야 R&D 이슈

- ETRI 정보보호연구본부(2022)에서 수행한 사이버보안 분야 STEEP 분석을 통해 거시환경 변화와 이에 따른 사이버보안 분야의 이슈를 정리한 결과는 다음과 같음

[거시환경 변화 분석에 기반한 사이버보안 분야 R&D 이슈]



- (Social) '비대면 사회'의 확산으로 인해 재택근무 및 원격교육이 보편화되고, 각종 사회시스템이 무인화되는 트렌드가 더욱 강해질 전망이며, '데이터 경제' 시대의 도래로 개인 프라이버시 보호 문제가 부각되고, 데이터 전주기 관리에 대한 요구가 강화될 전망
- (Technological) 제4차 산업혁명의 가속화로 '초연결'. '초지능', '초실감' 기술의 진화가 빨라지고, 이를 기반으로 새로운 '디지털 플랫폼'들이 보편화되며, '양자 컴퓨팅' 시대의 도래가 가시화될 전망
- (Economic) 디지털 전환 현상의 보편화로 '전산업의 디지털화'가 촉진되고, 디지털 기술 기반의 '데이터 경제 시스템'이 확산될 전망
- (Ecological) 전지구적 문제로 부각 중인 지구 온난화 및 환경 오염 문제들로 인해 '탄소중립' 이슈가 국가적으로 중대한 정책 이슈화되었으며, 이로 인해 '에너지 효율 컴퓨팅 환경'에 대한 요구도 증대
- (Political) '국가 공급망 위협' 우려가 심화되고, '사이버 범죄'가 고도화되면서 사이버 보안 문제는 이미 국가·기업의 생존과 관련된 정책적 이슈로 자리매김

Ⅰ 사이버보안의 개념 및 중요성

1 사이버보안 개념 및 범위

- **사이버보안(Cyber Security)에 관한 개념은 학술적으로 통일되거나 일관성 있게 합의되지 않은 채 사용되고 있으며, 국제기구와 국가별로 사용 용어 다소 상이**
  - 사이버보안은 사이버공간에서 발생하는 공격으로부터 정보, 정보시스템 및 정보통신망을 보호[1]하는 활동을 의미
  - 용어상으로는 '사이버안전', '사이버안보' 등이 사이버보안과 유사한 의미로 쓰이고 있으며, 기술적으로는 '정보보호', '정보보안'의 개념과 혼재되어 사용
    - · (사이버안전) 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태[2]
    - · (사이버안보) 사이버공간에서의 위협이나 공격으로부터 자국의 국민, 영토, 주권을 안전하게 보호하는 활동[3]
  - 국제사회에서 통용되는 용어 간 표현의 차이는 있으나, 공통적으로 '사이버공간에서의 위협으로부터 보호하는 활동'을 포함[4]하고 있음
    - · (미국) 정보가 내장된 컴퓨터, 전자통신시스템, 전자통신서비스, 유선통신 및 전자통신에 대한 피해 예방, 보호와 복구
    - · (독일) 독립적인 네트워크와 정보 인프라 등에 해를 끼칠 수 있는 위협으로부터 사이버 도메인을 보호하기 위해 사용될 수 있는 안전보장 장치 및 행위
    - · (EU) 독립적인 네트워크와 정보 인프라 등에 해를 끼칠 수 있는 위협으로부터 사이버 도메인을 보호하기 위해 사용될 수 있는 안전보장 장치 및 행위
    - · (ITU) 사이버 환경 및 기구 그리고 사용자의 자산을 보호하기 위하여 사용될 수 있는 툴, 정책, 안보개념, 안보보장장치, 가이드라인, 위험관리접근, 행위, 훈련, 모범사례, 보장 및 기술의 모음

- **사이버보안 용어에 관한 합의를 통해 유사 용어 사용 및 기술 계위에 관한 혼란 방지와 사이버보안 대응력을 제고할 필요가 있음**
  - 〈표 1-1〉과 같이 「국가기술표준분류체계」 및 「IITP 기술로드맵 2025」 등 국내 ICT 기술분류체계 상 사이버보안을 별도로 구분하여 명시하고 있지 않음

---

1) 한국법령정보원(2018), 사이버안보법제 고찰
2) 국가사이버안전관리규정(2013). 대통령훈령 제316호(2013.9.2. 개정). 제2조의 3
3) 한국법령정보원(2018), 사이버안보법제 고찰
4) 스위스 정부가 사이버보안 관련 정보수집을 위해 2014년 설립한 Global Cyber Definitions Database (http://cyberdefinitions.newamerica.org) 조사 결과

표 1-1 정보보호 기술 분류체계

구분	국가과학기술표준분류체계	IITP 기술로드맵 2025
정보보호	공통 보안기술	공동기반 보안
	네트워크 시스템 보안	시스템·디바이스 보안
	서비스/응용보안	네트워크·응용서비스보안
	산업보안/융합보안	물리보안
	달리 분류되지 않은 정보보호로 구성	융합보안

※ 출처: 국가과학기술표준분류체계, IITP 기술로드맵 2025(2020)

- 명확하게 구분되지 않는 사이버공간의 경계와 복잡한 사이버위협 등의 특성으로 사이버보안에 대한 개념 정립이 어렵지만, 체계적인 대응을 위해 용어에 관한 합의 필요

● **초기 사이버보안은 '정보보호'와 '정보보안'의 하위개념으로 분류해 왔으나, ICT 기술의 발달로 사이버공간이 확장되고 사이버보안의 중요성이 커짐에 따라 현재는 '정보보호' 및 '정보보안'과 동일계위로 간주하는 추세**

- (정보보호) 암호, 인증, 인식, 분석/감시 등의 보안기술이 적용된 제품을 생산하거나, 관련 보안기술을 활용하여 개인·기업·국가의 안전과 신뢰를 보장하는 서비스를 제공하는 기술[5)]
  - · (정보보안) 해킹, 데이터 유출로부터 PC·네트워크를 보호하며 ◁ 공동기반 보안, ◁ 네트워크 및 응용서비스 보안, ◁ 시스템·디바이스 보안을 포함
  - · (물리보안) 안전·안심 생활을 위한 재난·범죄 방지 기술로 ◁ 휴먼·바이오 인식 기술, ◁ 지능형 CCTV·무인전자 감시기술이 대표적
  - · (융합보안) 정보통신기술과 타 산업 기술 융합 환경의 보안기술로, ◁ 스마트 홈·빌딩 등 생활분야, ◁ 자동차·선박·해양·비행체·항공 등 이동체 분야 ◁ 헬스케어, 로봇 보안 등 다양한 분야와 결합
- 사이버보안 시장 및 기술개발 현장에서는 사이버보안을 '정보보호', '정보보안'과 동일한 개념으로 간주하고 있음

● **사이버위협의 다변화로 기존의 정보·물리·융합보안의 경계가 모호하고, 사이버보안의 범위와 영향력이 확대됨에 따라 사이버보안을 정보보호의 전체 영역으로 확장할 필요가 있음**

- 대표적인 물리보안 기술인 '지능형 CCTV'에서 사이버보안이 중요 이슈로 부각하고, 전산업 분야에서 사이버공격 위험성이 증가하는 등 정보보안, 물리보안, 융합보안의

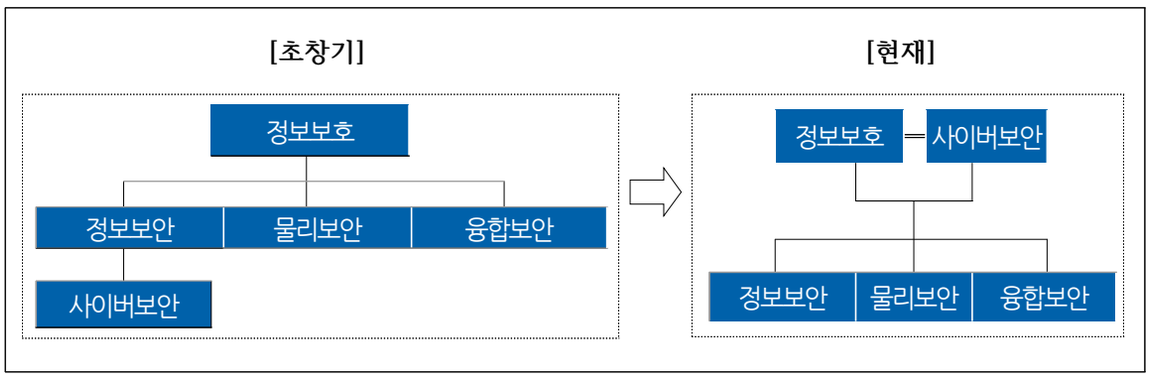
5) IITP(2020), ICT R&D 기술로드맵 2025

경계가 불분명해지는 추세

- 디지털 전환과 ICT 융합산업·서비스 확산으로 시장과 기술의 구분 및 경계는 더이상 무의미

- **이에 본 연구에서는 사이버보안에 관한 공통의미와 시장 및 현장성을 반영하여 사이버보안을 '정보보호', '정보보안'과 동일한 개념으로 간주하고, "사이버공간에서의 위협으로부터 개인·기업·국가의 안전을 보호하는 정보보호 기술"로 정의하고자 함**

그림 1-1 사이버보안 기술 개념의 확장



2 사이버보안의 중요성 및 국가투자전략 연구의 필요성

가. 디지털 전환의 가속화로 사이버 위협 증대

- **디지털 경제(digital economy) 성장과 디지털 전환(digital transformation) 가속화는 사이버보안 관련 광범위한 수요를 촉발**
  - 팬더믹 이후 재택근무 및 원격수업

  확대 등의 생활환경 변화와 비대면 경제 활성화로 디지털경제가 급성장
  - AI, 5G, IoT 등 첨단 디지털 기술의 급속한 발전과 새로운 디지털 기반 플랫폼 이용 확대로 디지털 전환이 빠른 속도로 진행
  - 모바일 기기 보급 확대, 기기 간 연결성 확장 등으로 사이버 해킹, 바이러스, 보안 패치, 기술 유출 등 다양한 디지털 사이버위협에 직면
  - 가속화되는 경제·사회 전반의 디지털화는 사이버보안 관련 다양한 이슈를 야기

- **AI 기반 자동화 등 신기술을 이용한 사이버공격력의 지능화·다양화·고도화**
  - AI와 사이버공격의 접목으로 사이버위협 유형은 더욱 지능화되고, 공격적 양상으로 진화·발전 중
  - 딥러닝 분석을 통한 정교한 공격과 자동화에 따른 고속화로 공격 범위와 피해 확대
  - 일반산업과 ICT 융합 확대로 전체 산업 분야가 사이버위협의 대상이 되어 산업·경제적 피해 심화*

    *2025년까지 사이버테러로 인한 글로벌 피해액은 10조 달러를 상회할 것으로 전망(Cybersecurity Ventures의 사이버범죄 연차보고서)

나. 사이버 피해의 심각화로 국가안보 관련 중요성 증대

- **IoT 기기, 드론, 자율주행차 등에 대한 사이버공격은 생명의 위협으로 직결**
  - 4차 산업혁명으로 촉발된 기술 진전과 융합으로 AI, IoT 기기뿐만 아니라 자율주행 자동차·스마트홈 디바이스 등 모든 사물과 환경이 해킹의 대상
  - 병원시스템 마비로 환자가 사망하거나, 교통수단에 대한 해킹으로 인적 손실이 발생하는 등 사이버위협은 인간의 생명을 표적으로 삼는 수준까지 발전

- **국가안보를 위협하는 파괴적 사이버위협 증가**
  - 국가기반시설에서 정보통신 기술과 서비스의 역할이 커지며, 전세계적으로 국가 주요 기반시설에 대한 사이버공격이 증가*하는 등 사이버위협의 경계 소실

* 국가 핵심 인프라 부문 조직에 대한 공격은 2013년 2건에 불과했으나, 2020년에는 399건에 달하며 급격히 증가(Gartner의 Cyber-Physical Systems Security 예측보고서)

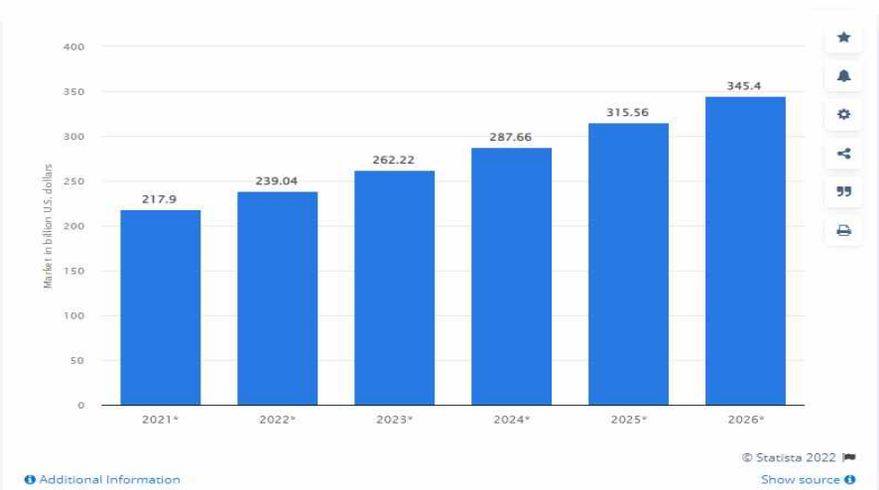
- 미국 콜로니얼 파이프라인(Colonial Pipeline)에 대한 랜섬웨어 공격('21.5)과 같은 국가 핵심 인프라 시설을 대상으로 한 파괴적 사이버 테러는 국가안보와 국민생명을 위협
  · 최근의 대규모 공격은 병원, 정부기관, 에너지 생성·송전시설 등 주요인프라를 대상으로 하고 있음

다. 정책 및 산업 관점에서 사이버보안 대두

- **국가 중요 인프라에 대한 보안은 전세계 정부의 주요 관심사로, 사이버공격에 대응하기 위한 안보 노력 강화**
  - 지능화되는 사이버위협으로부터 국가 중요 인프라 및 국민의 생명과 안전을 보호하기 위한 정부 차원의 대응을 강화하는 추세
  - 주요국은 관련 법률을 정비하고, 기술개발·인력양성 등을 위한 국가 예산 증대
- **사이버보안 글로벌시장 전망은 증가추세, 사이버보안의 중요성 커지며 시장도 성장**
  - 사이버 사기 및 범죄 빈도와 강도가 높아지며, 기업들은 자체 보안과 인프라 강화를 위한 첨단 정보보안기술에 투자 확대
  - 전세계 사이버보안 시장 규모는 2,179억 달러('21)이며, 연평균 성장률(CAGR, 2021-2026)은 9.7%로 2026년 3,453억 달러에 이를 것으로 전망

그림 1-2 전세계 사이버보안 시장 규모

단위 : billion U.S. dollars



※ 출처: Statista(2021)

- Gartner가 '2022년 12개 기술 트랜드' 중 2개 사이버보안 관련 이슈[6]로 선정할 만큼, 사이버보안 기술의 중요성 증대

그림 1-3 Gartner가 선정한 2022년 주요 기술 트랜드

Accelerating Growth	Sculpting Change	Engineering Trust
• Generative AI • Autonomic Systems • Total Experience • Distributed Enterprise	• AI Engineering • Hyperautomation • Decision Intelligence • Composable Applications	• Cloud-Native Platforms • Privacy-Enhancing Computation • Cybersecurity Mesh • Data Fabric

※ 출처: Gartner(2021)

라. 사이버보안 국가투자전략 수립을 위한 기반 연구의 필요성

- 사회 전반에 심각한 혼란과 교란을 초래하는 다양한 수법과 새로운 유형의 사이버 위협이 속속 등장하고 있음

- 사이버공격이 국가안보와 국민생명을 위협하는 수준으로 발전하면서 사이버보안 중요성은 날로 증대하고 있음

- 최근 우리 정부는 변화하는 환경에 맞춰 ◁ 데이터 산업 활성화 전략('18), ◁ 국가 사이버안보전략('19) 등의 사이버보안 정책을 마련하고, 관련 R&D 예산을 확대하고 있으나 아직 체계적인 국가투자전략과의 연계는 부족한 상황임

- 사이버보안 분야에 대한 국가적 차원의 전략적 중요성이 커짐에 따라 체계적·효율적인 국가투자전략 수립이 필요하며, 따라서 본 연구에서는 그러한 국가투자전략 의사결정에 필요한 정책/투자현황/기술/시장/산업/이슈 분석을 수행하고자 함

6) 사이버보안 매쉬 아키텍쳐와 개인정보 보호 강화 컴퓨팅이 사이버보안 관련 이슈에 해당(Top Strategic Technology Trends for 2022)

II 사이버보안 정책 및 투자 동향

1 주요국 사이버보안 정책 및 투자 동향

- 글로벌 주요국(◁ 미국, ◁ 중국, ◁ 일본 ◁ 유럽(EU, 영국, 독일))과 국내 사이버보안 관련 정부 정책과 투자 동향을 살펴보고자 함

- 사이버위협의 범위와 영향력이 커지고 국가안보를 위협할 만큼 고도화됨에 따라, 주요국은 주요 국정과제로 운영하며 독자적 사이버보안 전략을 수립
  - 사이버 위험을 국가위기관리체계에 포함하여 사이버보안 강화에 주력하고 있으며, 주요국의 사이버보안 관련 정책은 〈표 2-1〉과 같음

표 2-1 주요국 사이버보안 관련 정책 현황

국가		주요 정책	정책특징
미국		• 미국 국가 사이버 전략('18.9) • 국가 최상위 사이버보안 연구개발 전략계획('19.12) • 국가의 사이버보안 향상에 관한 행정명령('21.5)	사이버보안을 핵심 국정과제로 선정, 국가최상위 정책 수립하고 행정명령 발효
중국		• 국가 사이버공간안전전략('16.12) • 사이버안보 산업발전 3개년 행동계획안('21.7)	국가주도형으로 자국 이익 중심의 공격적 사이버보안 정책 전개
일본		• 사이버보안전략 2019-2021('19.9)	국가적 정책추진 방향을 반영하여, 3년 단위로 사이버보안전략 마련
유럽	EU	• 일반 개인정보 보호규정(GDPR) 및 NIS 지침 • 디지털 10년을 위한 EU의 사이버보안 전략('20.12)	데이터의 국가간 이동과 개인정보보호의 기반 마련
	영국	• 국가사이버보안전략 2016-2021('16)	주변국 파트너십과 국제협력 중요성 강조
	독일	• 독일을 위한 사이버보안전략 2016-2021('16)	국가안보 중심의 사이보보안정책 추진
한국		• 국가사이버안보전략('19) • 제 2차 정보보호산업 진흥계획('20) • 정보산업의 전략적 육성방안('22)	사이버보안의 핵심 지능정보기술 개발 확대 및 융합보안 강조

- 데이터의 국가 간 이동 및 개인정보보호 등이 주요 이슈로 등장, 미국 중심의 서구 자유주의 국가와 중국을 비롯한 비자유주의 국가 간 입장 차 존재
  - (데이터 이동) 미국, EU 등 서구 자유주의 국가들은 데이터의 자유로운 이동을 허용하는 입장인데 반해, 중국을 비롯한 비서구 비자유주의 국가들은 속지주의적 관점으로 접근
  - (개인정보 보호) 미국, 일본, 한국 등은 개인의 권리와 표현의 자유를 기반으로 하는 '사생활 보호'를 중시하고, 중국과 독일은 국가안보를 우선하는 규제정책 시행

- **미중 기술패권전쟁이 사이버보안 영역으로 확장, 자국 중심의 글로벌 거버넌스 도모**
  - 미국은 중국을 견제하며 동맹국과의 사이버보안 파트너십을 강화하는 협력 전선 구축
  - 중국은 자국을 중심으로 글로벌 진영을 확장하며 미국의 사이버패권에 대항
- **글로벌 주요국은 R&D 우선순위에 사이버보안을 포함하여 전략적으로 육성**
  - 한국을 비롯한 주요국은 사이버보안을 정부의 중점 R&D 영역으로 선정하고, 관련 산업을 육성
  - 사이버보안 관련 첨단 기술개발과 경쟁력 강화를 위한 국가 예산 투입 확대

표 2-2 주요국 중점분야 선정 현황

국가	주요 현황	관련 근거
미국	• 국가 R&D 중점지원 분야 • 10대 첨단기술 분야	FY 2030(Fiscal Year 2030) 끝없는 프론티어 법안
중국	• 디지털경제발전을 위한 8대 중점업무	14.5 디지털경제발전 규획
일본	• 국가 ICT R&D 4대 중점영역	제6기 과학기술기본계획
EU	• 6대 중점투자 분야	Horizon Europe 2020
한국	• 10대 국가필수전략기술	국가 필수전략기술 선정 및 육성·보호전략

- **국가차원 전략 수립과 함께 사이버보안 전담기관을 설치·운영하고, 전담조직의 권한을 강화하는 방향으로 발전**
  - 주요국은 법률 제정 등을 통해 사이버보안 전담기관의 설치와 운영 근거를 마련하고, 이들 기관에 사이버보안 관련 실질적인 권한을 부여
  - 미국과 중국은 국가 최고 리더십 단위에서 사이버보안 정책을 총괄
  - 유럽 주요국은 EU 전담기관인 ENISA가 EU 및 회원국의 정책 수립과 이행을 지원

표 2-3 사이버보안 관련 주요국 정부 거버넌스

국가		총괄 기능	전담기관	특징
미국		• 백악관 산하 국가안보위원회	사이버보안국(CISA)	백악관이 컨트럴타워 기능
중국		• 주석 산하 인터넷안전정보화위원회	국가인터넷정보판공실	주석 중심 중앙집권적
일본		• 총리 산하 사이버보안전략본부	내각 사이버보안센터(NISC)	사이버기본법을 통해 기능 역할 명확화
유럽	**EU**	• EC 산하 네트워크콘텐츠기술총국	사이버보안기관(ENISA)	ENISA 권한 강화 방향으로 발전
	영국	• 내각부	사이버보청(OCSIA)	범정부 컨트롤트워 기능 부재
	독일	• 내무부	정보기술보안청(BSI)	정부기관 영역별 소관업무 관장
한국		• 국가안보실	국가정보원	정부기관 분야별 업무수행

- **주요국은 사이버보안 관련 법률 제정을 통해 정부 정책과 제도를 뒷받침**
  - 주요국이 기본법률 제정을 통해 사이버보안 관련 제도 정비 및 대응체계를 마련하고 있는데 반해, 한국은 사이버보안법 부재 상황

표 2-4 주요국 사이버보안 관련 법률 현황

국가		사이버보안 관련 대표 법률
미국		• 사이버보안법(Cybersecurity Act)
중국		• 국가보안법(Law of the People's Republic of China on State Security) • 사이버보안법(Cyber security Law of the People's Republic of China) • 데이터보안법(Data security Law of the People's Republic of China)
일본		• 사이버보안기본법(サイバーセキュリティ基本法)
유럽	EU	• 일반개인정보보호규정(GDPR) • 정보보호지침(NIS)
	독일	• IT 보안법
한국		• 국가사이버 안전관리 규정

- **사이버공격에 대한 효과적 대응을 위해 공공과 민간의 정보 공유 및 협력 강화**
  - 민·관이 함께 사이버위험 정보를 공유하며 사이버공격에 대응
  - 정부는 민간의 투자를 유도하며 공적 자금 투입 최소화와 민간의 기술력 강화를 도모

표 2-5 주요국 민·관협력 강화 사례

국가		주요 정책
미국		• 공공과 민간 전문가가 함께 사이버보안 대응 논의 법제화 • 공공과 민간의 협업을 통해 사이버보안 인증 프로그램 개발
일본		• 공공과 민간의 이해당사자들 간 협의체를 통해 정보 공유 및 정책적 의사결정 관행 정착
유럽	EU	• 사이버보안 분야 민·관 프로젝트 추진
	영국	• 구글, MS 등 글로벌 ICT 기업과 공동투자로 사이버보안 솔루션 개발
	독일	• 독일 사이버보안 전략 2016, 사이버 위협 시 정보 공유와 협력의 중요성을 강조
한국		• 기본계획 제정 시 민간 협의체 운영 • 민·관의 전략적 협력을 위한 K-사이버보안 대연합 출범

가. 미국

- **미국은 사이버보안 세계 최강국으로, 9.11 테러('01) 이후 보안 강화 정책을 추진**
  - 디지털화에 따른 국익과 경쟁력 향상 이면에 보안 관련 문제 급증으로 대응책 마련 시급
  - 「국토안보법(Homeland Security Act)」을 제정하고, 전담부처인 '국토안보부(DHS, Department of Homeland Security)'를 신설('02)하며 대응체계를 마련
  - 테러공격 대응용 '사이버공간 확보를 위한 국가전략(National Strategy to Secure Cyberspace)'을 발표('03.2)하고, 국가차원의 최초 종합계획인 '사이버안보 대응책(Comprehensive National Cybersecurity Initiative)'을 수립('08.1)하며 사이버보안 정책을 점차 강화

- **백악관이 사이버보안 컨트롤타워 기능 수행, 대통령 중심으로 사이버보안 업무체계를 일원화**
  - 오바마 정부 출범('09) 이후 백악관이 직접 사이버보안을 비롯한 국가 전체 네트워크 안전 정책을 수립, 사이버보안 관련 정보 및 업무가 통합 관리되어 대통령에게 전달
  - 국가안보위원회(National Security Council) 산하 사이버보안국(Cybersecurity and Infrastructure Security Agency)이 관련 정부부처·산하기관과 협력하며 정책의 일관성과 대응체계의 기민성 발휘

- **사이버보안을 핵심 국정과제로 선정, '국가 최상위 정책'을 수립하고 행정명령을 발효**
  - '사이버보안법(Cybersecurity Act)'을 제정('15)하고, '사이버보안 관련 국가행동계획(Cybersecurity National Action Plan)'을 발표('16)
    - · 국가적 사이버보안 강화를 위한 조직 개편과 실천적 행동계획으로, 글로벌 차원 협력을 도출하기 위해 국무부가 핵심적 외교 노력과 산업증진 프로그램을 주도한 것이 특징
  - '국가 주요기반시설의 사이버위협 대응 강화를 위한 행정명령('13.2)*을 시작으로, '연방 네트워크 및 핵심 인프라의 사이버보안 강화에 관한 행정명령('17.5)**', '국가의 사이버보안 향상에 관한 행정명령***'에 서명('21.5)

    * 국립표준기술연구소는 사이버보안 프레임워크(Cybersecurity Framework)를 최초로 개발

    ** 연방기관의 네트워크 보안과 주요기반시설의 사이버보안을 강화하는 것이 주요 골자

    *** 정부 주도의 사이버공격 대응과 민간협력을 통한 사이버공간 육성을 강조, 대규모 사이버공격에 대한 신속대응과 NIST(National Institute of Standards Technology), CISA 등의 새로운 사이버보안 기관 창설
  - 백악관은 '미국 국가 사이버 전략(National Cyber Strategy of the United States of

America)*'을 발표('18.9)하고, '국가 최상위 사이버보안 연구개발 전략계획(Federal Cybersecurity Research and Development Strategic Plan)**'을 수립('19.12)

* 행정명령('17)을 토대로 연방 네트워크 및 주요기반시설에 대한 사이버보안 강화의 기술발전 청사진을 제시하고, 사이버공격자에 대한 정부 대응 권한을 강화한 것이 특징

** 사이버보안 내 인간 역할 증진과 지속가능한 사이버보안 시스템 개발 등의 국가 행동계획을 명시

- 바이든 정부는 중요한 기반시설 제어 시스템을 위한 사이버보안 국가 안보 각서(National Security Memorandum)에 서명('21.7)
  - · 사이버보안이 국가적 중대 사안임을 재피력하는 한편, 국가 핵심 인프라 운영자의 사이버보안 관련 준수사항을 명시

● **각 부처는 사이버보안 국가 최상위 전략의 세부계획과 사업 추진하며, 정책 실효성을 뒷받침**

- 정부조직은 부처 특성에 맞춰 '미국 국가 사이버 전략' 실행 세부계획을 마련('18.5)
  - · 에너지부가 가장 먼저 '에너지 부문 사이버보안을 위한 계획' 수립('18.5)하고, 국토안보부와 국방부는 부처별 '사이버보안전략' 수립('18.9), 사이버공격의 영향 완화 등을 위한 향후 5년의 수행전략 제시
- 에너지부, 사이버위협으로부터 전력 운영 보호를 위한 조치 시행('21.4)
  - · 에너지부는 미국 전력 시스템에 대한 사이버보안 위험을 해결하기 위한 100일 계획을 시작, 미국 중요 에너지 기반시설 보호를 위한 첨단기술 사용과 이해 관계자 의견 수렴[7)]
- 국토안보부, 최초의 파이프라인 사이버보안 강화명령 조치('21.5)
  - · 국토안보부는 파이프라인 해킹사태 재발 방지를 위해 사이버보안 강화 명령을 내리고, 사이버보안 전담 담당관 24시간 배치 등을 의무화

● **미중 기술경쟁에서 사이버보안 강화하며 중국 견제, 국가 간 전략적 파트너십 활발히 전개**

- 트럼프 정부 출범('17) 이후 중국 견제를 위한 글로벌 동맹 전선을 구축하고, 사이버보안 정책을 한층 강화
  - · NASA는 사이버공간에서 중국, 러시아 등의 안보 위협에 대처하기 위한 자체 사이버보안국 신설
- 사이버보안 관련 개별 기업과 국가 단위 협력을 확장하여 국제 관계에서의 전략과 파트너십을 추진, 특히 호주, 인도와 함께 사이버보안 파트너십을 강화
  - · 동맹국을 중심으로 클린네트워크 프로그램(Clean Network Program) 추진(2020), CNP는 데이터 프라이버시(data privacy), 안보(security), 인권(human rights)을 보장

7) Department of energy(2021), Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats, APRIL 20, 2021

- **민·관 협력체계를 구축하고, 국가 기간산업으로서의 가치를 강조**
  - 국가 사이버보안 증진위원회는 선도적 기술기업 CEO, 입법부, 사법부 전문가 등과 함께 공공과 민간분야 사이버보안 강화방안 및 세부사항을 논의하도록 법제화
    - · 국토안보부는 민간과 함께 사이버보안 인증 프로그램 개발 등의 민·관 협력체계 마련
  - 국가 핵심 인프라 시설에 대한 사이버위협으로, 미국의 사이버보안은 단순 산업 영역을 벗어나 국가안보와 국민생명이 직결된 국가 기간산업으로서 가치를 강조하는 추세
- **R&D 우선순위 등 집중 지원 분야로 선정하며 사이버보안 중요성 강조**
  - FY 2030(Fiscal Year 2030)은 R&D 우선투자 분야에 국가안보를 위한 사이버보안 기술을 선정('21.8)
    - · 국방, 사이버보안, 인프라 안전 등 안보 관련 R&D 투자와 AI, 퀀텀 컴퓨팅, 5G, 첨단제조업 등 차세대 기술에 대한 투자를 확대
  - 끝없는 프론티어 법안(Endless Frontier Act)에서는 사이버보안 관련 기술을 R&D 집중 지원이 필요한 10대 첨단기술 분야 중 하나로 선정
    - · 사이버보안 관련 기술(데이터저장, 데이터 관리기술)에 5년 동안 1,000억 달러 투입 계획을 명시
- **연방정부는 미국 사이버보안 시장의 최대 투자자로, 정부 예산은 꾸준히 증가**
  - 미국 대통령 예산안에서 사이버보안 관련 예산은 매년 확대

표 2-6 미국 연방정부 사이버보안 예산 현황

회계연도	FY 2018	FY 2019	FY 2020	FY 2021
예산액	149.78억 달러	166.45억 달러	174.35억 달러	220억[8]

※ 출처 : IITP(2019), KOTRA(2018) 자료를 토대로 저자 정리

  - 연방정부는 미국 사이버보안 시장의 최대 투자가이자 소비자로서, 미국 전체시장의 58.8%에 해당하는 연간 140억 달러의 예산을 집행하며 관련 산업과 기술을 선도

- 미국은 사이버보안 원천기술과 R&D 경쟁력을 확보한 세계 최강국으로, 조기에 사이버보안을 핵심 국정과제로 선정하고 집중육성
- 대통령 중심의 사이버보안 업무체계 일원화로 정책의 일관성과 대응의 기민성 확보
- 사이버보안을 강화하며 미중 기술경쟁에서 중국을 견제하는 국제전략 표방
- 연방정부는 미국 사이버보안 시장의 최대 투자자이며, 정부 예산을 확대하며 기술과 산업을 육성

8) Market Research Media는 연방정부의 사이버보안 예산이 2022년 220억 달러에 달할 것으로 전망함

나. 중국

- **중국은 국가주도형 거버넌스의 대표국가로 속지주의 관점[9]을 기반으로 공격적인 사이버보안 정책을 추진**
  - 데이터 및 개인정보의 현지 저장(Data Localization)을 의무화하고, 반 정치체제적인 콘텐츠는 유포를 금지
  - 중국 내 데이터의 해외 유출을 저지하는 등 사이버공간에 대한 전 방위적 규제를 추진하고, 사이버공격에 대한 보복을 허용하는 '능동적 방어 전략'을 견지
- **국가주석 중심으로 사이버보안을 총괄하며 중앙집권적 체계로 운영**
  - 시진핑 정부 출범('13) 이후 사이버보안 중요성 피력, 사이버보안을 총괄하는 최고 정책결정기구 '중앙인터넷안전정보화위원회' 설치('14)
  - '국가인터넷정보판공실'이 중국정부의 지침을 전달하고 각 부처가 이행하는 구조로 운영
    - · 국가인터넷정보판공실은 '국가 정보보보호 사고 응급대응계획('17.6)', 정보보호 인재 양성을 위한 '일류네트워크안전학원 육성계획('17.8)' 등 다양한 사이버보안 시행계획 발표
- **중국 최초의 사이버보안 국가전략 '국가 사이버공간안전전략'을 발표하며, 사이버보안이 국정의 전면으로 등장**
  - 국가차원에서 정식으로 채택('16.12)한 첫 사이버보안 전략으로, 주권 수호와 국가 안전 보장, 사이버 위법 행위 엄벌, 사이버공간 국제협력 강화 등을 골자로 하는 9개의 주요 전략적 임무*를 제시
    - * ◁ 사이버공간의 주권 보호, ◁ 국가안전 수호, ◁ 주요정보기반시설 보호, ◁ 사이버문화 건설의 강화, ◁ 사이버테러 및 범죄 단속, ◁ 사이버 관리체계 고도화, ◁ 사이버보안 기초의 확립, ◁ 사이버공간 방어능력의 향상, ◁ 사이버공간의 국제협력 강화
- **'14.5 디지털경제발전 규획('22.1)'에서 디지털경제 발전을 위한 8대 중점업무로 '사이버보안 강화' 포함**
  - 사이버보안 및 데이터보안 강화와 각종 리스크의 효과적인 예방을 위한 조치를 명시
- **미국의 사이버 패권 대항 및 글로벌 사이버 거버넌스를 견제하는 국제협력전략 전개**
  - 자국 중심의 사이버 거버넌스 진영을 구축하고 국제협력 강화를 위해 최초로 국제적 사이버보안 전략을 명시한 '사이버공간 국제협력 전략'을 발표(17.3), 사이버공간의 국제질서 구축을 위한 UN과 국제사회의 역할을 강조
  - 미국과의 협력을 시도하고 있으나, 미국의 '자유로운 정보 유통'과 중국의 '국가안전

9) 사이버공간을 육해공과 같은 기존 주권국가의 담당지역으로 보는 관점

우선주의' 충돌 등 미중간 근본적 입장차로 마찰이 불가피한 상황

- 미중 간 전략적 경쟁과 통상 마찰 장기화에 따른 중국의 EU 의존도 상승하며, 지적 재산권 보호를 포함하여 사이버공간의 위협 활동에 대한 협력과 공동대응에 합의

● **사이버보안 관련 3대 주요 법률을 근거로 사이버보안 정책 및 제도 추진**

- '국가보안법(Law of the People's Republic of China on State Security)'
  - · '15년 7월에 발표된 중국 사이버보안법의 근간이 되는 법률로서, 국가 주권의 범위를 사이버공간으로 확장하여 사이버공간에 대한 중국의 주권 행사를 명문화
- '사이버보안법(Cyber security Law of the People's Republic of China)'
  - · 핵심 정보 기반시설 보호와 온라인 실명제 도입, 개인정보보호 등을 총망라한 법률로서 종합적인 규제 프레임워크 마련, '17년 6월 부분 시행(데이터 보안 관련 조항 유보) 후 '19년 1월 전면시행
  - · 국외기업의 검열과 내부 사이버 공간 통제, 모든 네트워크 대상에 대한 사이버 사고관리제도·보안등급 보호제도·제품 및 서비스의 인증을 의무화함으로써, 국적에 상관없이 중국 내 데이터 수집·운영·유지 기업은 모두 사이버보안법을 준수
- '데이터 보안법(Data security Law of the People's Republic of China)'
  - · 데이터를 취급하는 기업에 대한 규제 강화를 위해 '21년 9월 전면시행되었으며, 중국 내에서 수집·생성한 중요 데이터의 역외 이전을 통제와 위반 시 강력한 처벌이 주요 골자
  - · 중국 정부가 포괄적 거버넌스 시스템을 통해 데이터를 집중단속하고 국가 사이버보안 장벽을 구축하겠다는 의도 내포[10)]

● **사이버보안 산업발전과 시장확대를 위한 투자 증대**

- 중국 공업신식(정보)화부는 '사이버안보 산업발전 3개년(2021~2023년) 행동계획안('21.7)'을 통해 사이버보안 산업시장 3년 내 44조 규모의 육성계획 발표
  - · 3년간 연간 15% 이상 성장 목적으로 정보화 분야의 10%까지 사이버보안 중점산업에 투자

- 대표적인 국가주도형 거버넌스 정부로, 사이버 주권수호와 내정불간섭 원칙 견지
- 국가 주도 하에 국민과 기업에 대한 강력한 통제력 행사
- 자국 플랫폼 기업 독점은 보호하고, 외국기업 규제를 강화하는 공격적 행보
- 중국을 중심으로하는 글로벌 거버넌스로 미국을 견제하는 국제협력 전략 채택

10) 조선일보(2022), 경제분야 극단 美中, 사이버보안 영역으로 전쟁 확대

다. 일본

- **일본은 주변국의 대규모 사이버테러와와 개인정보유출 사고 등을 목격하며, 본격적인 사이버보안 전략을 마련하기 시작**
  - '06년부터 매 3년 단위 '정보보호전략'을 발표하고 있으며, 2013년부터 '사이버보안전략(Cyber Security Strategy)[11)]'으로 개명
  - 국민을 지키는 정보보안전략(2010-2012) : 사전예방뿐만 아니라 사후처리 중요성을 인식하기 시작하며 '사고 전제 사회' 관점으로 전환
  - 사이버보안전략('13-'15) : 내각 사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity) 설립 추진
  - 사이버보안전략('16-'18) : 일본연금기구 해킹사건에 대한 정부 대응 지연을 계기로 내각 사이버보안센터 기능을 강화, 조사 및 감시대상을 정부뿐만 아니라 독립행정·특수법인까지 확대
  - 사이버보안전략('19-'21) : 사이버보안 투자 확대, 민·관협력을 통한 정책 추진, 도쿄올림픽을 대비하는 보안대책 강화
- **'사이버보안 기본법' 제정을 통해 사이버보안 추진체계를 뒷받침**
  - 사이버보안 최초 법률인 '사이버보안 기본법'을 제정('14.11), 사이버보안 강화를 공개 천명하고 관련 정책을 추진
  - 기본법을 통해 사이버보안전략 수립 및 사이버보안전략본부와 내각의 사이버보안센터 설치의 근거를 마련
  - 국가가 사이버보안 책무의 주체임을 명확화하고, 관련 기관의 권한을 명시
- **총리 산하 '사이버보안전략본부'가 컨트롤타워 기능을 담당하고, 산하조직 '내각 사이버보안센터'가 전담지원기관 역할 수행**
  - 사이버보안전략본부는 내각관방장관이 총괄 지휘하며 사이버보안 관련 학계 및 업계의 전문가들로 구성, 직할 조직으로 내각 사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity) 설치·운영
  - 전담조직을 통해 사이버보안 정책 수립의 전문성이 제고되고, 사이버공격 시 국가 역량 결집과 대응력이 향상
  - 방위성과 자위대는 사이버 국방, 외무성은 사이버 국제협력, 경제산업성은 IT 산업 정책, 총무성은 통신 및 네트워크 정책, 경시청은 사이버범죄 대응 등의 분야를 맡아 실무부처 차원에서 소관 업무를 실행

11) 사이버보안기본법에 의거, 향후 3년간 사이버보안 정책 내용을 수립하여 국회에 보고하도록 의무화

- **공공과 민간의 이해당사자 간 협의체를 통해 전략적 대처방안 제시**
  - IoT를 활용하는 민간기업의 해외시장 경쟁력 확보를 위해 사이버보안의 중요성을 강조하며, 산·학·관이 참여하는 'IoT 컨소시엄'을 설립('15)
  - 각 부처 사이버보안 관련 조직과 민간의 관련 당사자들이 사이버위협 정보를 공유하고 의사결정하는 협력의 관행 정착, 협의체 역할과 비중을 강화하는 추세

- **미국과의 사이버보안 협력을 강조하며, 주변국과 사이버정책 대화 등을 통해 다자외교 추진**
  - 전통적 우방인 미국의 사이버보안 능력을 활용하여 일본의 사이버안전을 보장받는 '사이버 우산' 전략을 견지
  - 주변국 호주, 영국, 프랑스, 한국 등과 사이버 정책 대화 등을 통해 다자외교 추진*

    * 미국, 호주, 인도 등의 중국 견제 동맹체인 쿼드(Quadrilateral Security Dialogue) 및 동남아시아 국가연합(Association of Southeast Asian Nations)과의 다자간 사이버보안 협력을 강조

- **국가 ICT R&D 4대 중점영역으로 선정, 관련 예산 꾸준히 증액하며 대응 강화**
  - 총무성은 사이버보안을 비롯한 AI, beyond 5G, 양자정보통신을 국가차원의 4가지 전략적 추진영역으로 선정, R&D 중장기 계획을 수립하고 투자확대

    · 총무성 산하 정보통신연구관(NICT) 연구예산에서도 사이버보안 분야는 안정적인 연구비 수준 유지
  - 일본 정부 사이버보안 예산 총액은 '18년 622.1억 엔에서 '19년 852.8억 1만 엔(약 9,451억 원)으로 전년 대비 약 27% 증가

표 2-7 일본 정부 사이버보안 예산 현황

회계연도	2015	2016	2017	2018	2019
예산액	325.8억 엔	498.3억 엔	598.9억 엔	622.1억 엔	852.8억 1만 엔

※ 출처 : ETRI(2022), 정부 ICT R&D 포트폴리오 분석

- 변화하는 환경에 대한 주기적인 검토를 통해 정부정책을 지속적으로 보완하며 개선
- 사이버보안을 국가 ICT R&D 중점영역으로 선정하여 투자를 확대하며 집중육성
- 전통적 우방인 미국과의 협력을 통해 자국안전 도모하는 '사이버 우산' 전략이 특징

라. 유럽

□ EU

- **EU의 사이버보안 전략은 '디지털 어젠다(Digital Agenda for Europe)' 중 '신뢰와 보안(Trust and Security)'에서 시작**
  - EU는 유럽의 디지털 어젠다('12)를 통해 국제적 사이버 공격의 예방과 대처를 위한 협력과 위험관리 체계를 마련하기 위해 정보 보안에 관한 지침을 제안
  - 2013년 '사이버보안전략(Cybersecurity Strategy of the European Union)' 최초 버전 채택, 사이버 복원력 강화와 사이버범죄 감소 등의 목표를 위해 회원국 정부 주도의 예방 및 대응수단 마련 민·관 협력체계 확립을 강조
  - 유럽네트워크정보보호원(European Network and Information Security Agency) 및 컴퓨터침해사고대응팀(Computer Emergency Response Team) 역할 강화와 '사이버 보안법'제정의 필요성을 강조

- **유럽 시장 분열과 장벽에 대한 위험 방지를 위해 '디지털 단일시장(Digital Single Market)'을 채택하며, 사이버보안 및 개인정보 보호 법규 개선 추진**
  - EC(EU 집행위원회)는 역내 디지털 경제활동의 제약요인을 제거하고, 하나의 시장형성을 목표로 디지털 단일시장전략을 채택('15.5)
  - 디지털 단일시장의 완전한 기능을 위해 네트워크 보안은 필수적으로, 유럽 디지털 산업 경쟁력 강화방안과 미래전략을 담은 '디지털전략 정책안*'을 발표('20.2)

    * 데이터단일시장 구성을 주요 내용으로 하는 유럽데이터전략(A European Strategy for Data)과 AI 기술의 윤리적 이용을 강조하는 인공지능백서(White paper on Artificial Intelligence)로 구성

- **'디지털 10년을 위한 EU의 사이버보안 전략(The EU's Cybersecurity Strategy for the Digital Decade)' 발표('20.12)**
  - 유럽연합 집행위원회(EC)는 ◁ 필수 서비스 및 인프라에 대한 보안 ◁ 사이버공격 대응을 위한 집단적 역량, ◁ 사이버공간 안정성 보장을 위한 전 세계 파트너십 강화를 골자로 하는 새로운 EU 사이버보안 전략을 마련

- **'일반 개인정보 보호규정(General Data Protection Regulation)' 과 정보보호지침(Network and Information Security) 도입('18), 사이버보안 전략 추진에 탄력**
  - (GDPR) 시민의 개인정보 활용 제한과 유출로 인한 사이버보안 위험 방지가 핵심으로 데이터의 국가 간 이동 및 개인정보의 보호 기반을 마련, 공공 및 회원국뿐만 아니라 민간부문 및 EU 사이버공간을 이용하는 국가까지 적용

- (NIS 지침) 주요기반시설 부문에서 '필수적인 서비스'를 제공하는 조직들이 네트워크 및 정보시스템에 대한 위협을 관리하는 세부적인 기술적 조치 제공
- GDPR은 개인정보 수집 조직에 초점을 맞추고 NIS는 주요기반시설 제공자의 복원력 강화에 중점, 유럽 회원국 및 회원국 내 역외기업에도 적용되며, 위반 시 과징금 부과 등의 처벌규정 명시

● **'EU 사이버보안법(Cybersecurity Act)' 시행('19)을 통해 사이버보안 강화**

- EU 공통 ICT 사이버보안 인증체제 도입과 유럽 보안 전담기관인 ENISA(European Union Agency for Network and Information Security)의 지위 영구화 및 유럽연합 전역의 인증 프레임워크 구축이 주요 골자
- 사이버보안법으로 사이버보안인증제도는 GDPR과 더불어 필수 인증 항목으로 인정

● **EU의 사이버보안 관련 정책은 네트워크콘텐츠기술 총국이 총괄**

- EU의 사이버보안전략은 EC 산하 '네트워크콘텐츠기술총국'(Directorate General for Communications Networks, Content and Technology)이 총괄하고 있으며, ENISA로부터 정책 및 기술 자문을 받고 있음
- ENISA가 EU 차원 정책 및 규정 개발, 회원국과 EU 소속기관 등의 자발적 정책 수립과 이행을 지원

● **사이버보안 분야 민·관 프로젝트(Cybersecurity Public-Private Partnership) 추진**

- 사이버복원력 강화와 산업 촉진을 위해 사이버보안 분야에 특화된 민·관 합작 프로젝트를 결성('16.7), 에너지, 의료, 교통, 금융산업을 위한 보안제품과 서비스 개발을 지원하는데 총 4억 5,000만 유로의 기금을 공동 부담
- 정부와 민간 공동투자로 사이버보안 연구개발에 공적 자금 투입을 최소화하고 민간의 사이버보안 기술력 강화 도모

● **다자간 조약인 '유럽 사이버범죄 방지협약'에 대한 국제적인 합의 확대 추진**

- 미국 등 동맹국 중심 클린네트워크 프로그램(CNP)에 참여('20), 미국 중심의 사이버 보안 전략을 국제적인 차원으로 확대하겠다는 의도 내포
- 제3국과 사이버 외교 네트워크 구축, 국가차원 해킹 방지 등의 국제협력 증진

● **최근 수립된 주요 ICT 정책에서 사이버보안을 핵심 유망기술로 선정하고 집중 투자**

- 'Horizon Europe 2020'은 보안 및 연결 외 6개 기술 분야*에 중점투자

  * 보안 및 연결, 첨단제조, 첨단 소재, 생명과학과 기술, 마이크로/나노전자 및 광자, 인공지능

- 'Digital Europe Program('21~'27)'에서 디지털 기술의 경쟁력 확보를 위해 사이버보안, 고성능 컴퓨팅,

인공지능 분야를 집중육성, 총 92억 유로 중 사이버보안에 20억 유로 투자 계획 명시

□ 영국

- **영국은 2009년 첫 '사이버보안 전략' 발표 후 'The UK Cyber Security Strategy('11)', '국가 사이버보안 전략(National Cyber Security Strategy) 2016('16)'을 순차적으로 마련**
  - 공공·민간·국제협력을 통한 안전한 사이버공간 구현 등 정부 단위 정책 방향 제시
  - 국가 주요시설 사이버공격과 테러 위협 차단을 위한 중장기 '국가 사이버보안 전략' 수립
    - · 사이버보안 예산 2배 확대('20년까지, 총 19억 파운드, 2.8조 원 규모), 세계시장에서 국립 사이버보안센터(National Cyber Security Centre) 역할 확대 등을 도모
- **영국의 사이버보안은 내각부에서 총괄, 해외 부문은 외무부가 주요 역할 수행**
  - 내각부는 산하단체 사이버보안청(OCSIA) 등을 중심으로 사이버보안 정책 수립 및 업무를 수행, 범정부 컨트롤타워 수준의 역할은 제한적
  - 해외 부문은 외무부 정보통신본부(GCHQ)가 주요 역할 수행, 국립사이버안보센터(NCSC)를 통해서 관련 기관들과 협력하는 체계로 운영
- **글로벌 ICT 기업과 민·관 협업을 통한 민간투자 유도**
  - 정부는 디지털 보안 내재화를 위하여 구글, MS와 약 1.9억 파운드(2,904억 원)를 공동투자하고, 민·관이 함께 향후 5년간 사이버보안 솔루션 개발 진행('19.8)
- **국제협력에 대한 중요성을 강조하며, 주변국과의 양자 협력 및 국제기구를 통한 파트너십 구축**
  - 영국은 2015년 미국과 사이버보안 역량 강화 프로그램에 합의하는 한편, 중국과 상호 간 사이버 첩보 활동 금지하는 사이버보안 협정을 체결
  - UN, G20, EU, NATO 등과 같은 기존의 국제기구와 다자외교 프레임워크를 활용하여 국제공조에 참여

□ 독일

- **독일은 국가안보를 중시하는 사이버보안 정책 전개**
  - 사이버보안 비중이 높은 국가 중 하나로 NATO 국가 중 처음으로 사이버 부대를 창설('09) 하는 등 사이버보안에 능동적으로 대처
  - 독일은 정보통신산업이나 프라이버시를 강조하는 EU 회원국 대비 상대적으로 주요 기반시설에 대한 사이버 방위에 더 많은 관심

- **연방 내무부가 '독일 사이버보안전략(Cyber-Sicherheitsstrategie für Deutschland)' 수립, 사이버공간 변화와 새로운 사이버위협에 대비하며 전략 수정**
  - 사이버보안전략('11) : 2005년 발표된 '정보기반시설의보호를위한국가계획'을 대체한 첫 사이버보안전략으로, 정부는 정책의 기본방향을 반영하여 5년마다 사이버보안전략 수립
  - 사이버보안전략 2016('16) : 하드웨어와 시설 보호 중심에서 개인과 기업 중심 보안으로 정책 이동, 사이버위협 시 공공과 민간 간의 정보 공유와 협력 강화의 중요성 강조
    - ◁ 디지털 환경에서 안전하고 독립적인 행동 보장, ◁ 국가-민간 간 협력, ◁ 효과적이고 지속가능한 사이버보안 아키텍처, ◁ 독일의 주도적 위상 확립을 독일 정부의 주요 추진전략으로 제시
  - 사이버보안전략 2021('21) : AI를 통한 IT 보안 확보 등 정보통신기술의 활용 및 중요성 강조, 사이버보안 분야 정부·기업·학계·시민사회 간 협력 강화
    - ◁ 사이버보안 정립을 위한 국가와 사회의 공동 의무, ◁ 디지털 주권, ◁ 디지털화의 성공을 위한 보안, ◁ 보안 정책의 투명성 강화 등 4가지 가이드라인을 중심으로 세부전략 발굴
- **연방정보보안청(Bundesamtes für Sicherheit in der Informationstechnik)이 사이버보안 정책 전반을 총괄하며 구심적 역할**
  - BSI가 기술 업무뿐만 아니라, 법적 임무 수행 지원 및 테러정보 수집 및 평가 등 광범위한 사이버보안 업무를 총괄·집행
  - 경제에너지부, 교육연구부, 국방부 등 정부 기관이 영역별로 사이버보안 소관업무 관장
- **'NIS 지침 시행법'과 '신 IT 보안법'을 통해 사이버보안 지탱**
  - NIS 지침 시행법('17) : EU NIS 지침을 독일의 국내법에 적용하기 위해 '17년 법안 발효, 기존 IT 보안법에서 규정하는 주요기반시설 외 의료, 금융, 보험, 운수, 교통 분야 관리 대상에 포함
  - 신 IT 보안법('21) : '21년에 제정된 신 IT 보안법은 '15년 도입된 연방정부 'IT보안법('15-'20)'의 2.0 버전으로, 사이버보안 관련 최초의 포괄적 프레임워크를 제시
    - ◁ 사이버공격 탐지 시스템 도입 및 입증 의무('23까지), ◁ 관련 부서의 권한 확대 및 연방의회에 대한 보고 의무, ◁ 사이버범죄 처벌강화, ◁ 네트워크 확장에서 개별 공급 업체를 제외할 수 있는 '화웨이 조항' 신설 등이 주요 골자
- **독일의 사이버 역량을 주변국에 지원하며 자국의 역할과 영향력 강조**
  - 주변국과 우호적 관계를 유지하며, 유럽 내 독일의 역할 확대 도모
  - 국가 단위보다는 유엔, EU, 나토, G8 등 다자기구와의 협력 강조하며 국제적 공조

- EU는 GDPR과 사이버보안법을 통해 데이터의 국가 간 이동과 개인정보보호 기반 마련
- 영국은 주변국 및 국제기구를 통한 파트너십 구축하며 국제협력 중요성 강조
- 독일은 국가안보를 중시하는 정책 경향, 사이버 역량 지원 통해 자국 영향력 확대 도모
- ICT 정책에서 사이버보안을 유망기술로 선정하고 투자를 확대

2 국내 사이버보안 정책 동향

- **한국은 2016년 범정부 차원의 첫 '정보보호산업 진흥계획'을 수립('16.6)**
  - '정보보호산업의 진흥에 관한 법률' 시행('15.12)에 따른 후속 조치로, 창업 활성화와 해외 진출 중심의 경쟁력 강화에 초점
  - 2015년 미래창조과학부가 'K-ICT 시큐리티 발전전략'을 발표한 바 있으나, 범정부 차원에서 마련된 첫 시행계획이라는데 의미가 있음

- **사이버보안 분야 최상위 지침서가 되는 '국가사이버안보전략'을 최초로 수립('19.4), 사이버보안 관련 정책을 재정비하고 구체화**
  - 사이버보안 정책의 최상위 지침서로, 국가 사이버안보의 미래 비전과 목표를 제시하고 개인·기업·정부가 중점 추진해야 할 전략적 과제*를 제시

    * △국가 핵심 인프라 안정성 제고, ◁ 사이버공격 대응역량 고도화, ◁ 신뢰와 협력 기반의 거버넌스 정립, ◁ 사이버보안산업 성장기반 구축, ◁사이버보안 문화 정착, ◁ 사이버안보 국제협력 선도
  - 국가차원의 첫 사이버안보 전략이며, 사이버공간을 국가가 수호해야 할 안보의 영역으로 인식하고 명문화
  - 국가사이버안보전략을 구체적으로 실행하기 위한 후속 조치로 '국가 사이버안보 기본계획 2019~2022'을 마련('19.9)

- **'제2차 정보보호산업 진흥계획' 수립('20.6), 사이버복원력 중요성 강조**
  - 범정부 법정계획으로 민·관 실무협의체 운영을 통해 제2차 정보보호산업 진흥계획('21-'25)을 수립하고, ◁ 디지털 전환에 따른 정보보호 신시장 창출, ◁ 민간주도 사이버 복원력 확보를 위한 투자확대, ◁ 지속성장 가능한 정보보호 생태계 조성을 중점 추진
  - 사이버공격의 예방보다 사이버 복원력의 중요성을 강조하고 있으며, 정부 정책 및 투자의 한계를 인식하고, 민·관협력 및 규제 완화를 통한 민간의 투자확대를 유도한다는 전략
  - 사이버위협에 대한 선제 대응을 위해 차세대 보안기술의 선점과 기초·원천기술개발 필요성을 강조

- **국가차원에서 반드시 확보해야 할 국가필수전략기술로 사이버보안 선정**[12)]
  - 글로벌 기술패권 경쟁 심화에 따라 국가차원에서 필수적으로 확보해야 하는 10대 국가필수전략기술로 '사이버보안' 선정*, 국가안보 차원에서 반드시 자국의 역량으로 기술확보가 필요한 분야로 인식

12) 「글로벌 기술패권 경쟁에 대응한 국가필수전략기술 선정 및 육성·보호전략」, 과기장관회의('21.12.22)

* 「글로벌 기술패권 경쟁에 대응한 국가필수전략기술 선정 및 육성·보호전략」, 과기장관회의 ('21.12.22)

- 사이버보안의 10대 국가필수전략기술 선정에 따라, '사이버보안 新기술 개발 로드맵'을 수립할 예정('22년 하반기)

- **'정보보산업의 전략적 육성방안' 발표('22.2), 새로운 보안 시장을 주목하며 관련 투자 확대**
  - 정보보호산업이 높은 성장률을 보이면서, 새로운 경제 성장 기회를 창출하는 국가 전략산업으로 인식
  - 인공지능·비대면·융합보안 등 새로운 보안 시장을 주목하고, 차세대 정보보호 기술 경쟁력 확보를 위한 투자확대*

  * 차세대 기술확보를 위한 정보보호 R&D 대폭 확대('21년 747억 원에서 '22년 928억 원으로 24% 증가)

- **대통령 산하 국가안보실에서 사이버보안 관리체계 총괄, 다수 정부 기관이 분야별로 업무 수행하는 분산형 구조로 국가차원 통합적 대응에 한계**
  - 공공과 민간부문별 주관부처가 있는 분산형 체계로, '국가사이버안전관리규정'에 의거, 국가정보원은 공공부문 사이버안전 관련 정책과 관리를, 과학기술정보통신부는 민간 부문의 사이버보안을 담당
  - 민간 정보통신 인프라 보호는 행정안전부, 정보보호 산업 육성은 산업통상자원부가 담당하며, 국가 주요기반시설의 경우 국가정보원, 국방부, 과학기술정보통신부가 분권적으로 대응

- **민·관 사이버보안 전반에 대한 전략적 협력, K-사이버보안 대연합 출범('21.11)**
  - 사이버공격의 진화로 기존의 분야별, 기업별 분절적인 대응에 대한 한계 인식, 사이버 공격에 대한 면밀한 방어체계 구축을 목표로 민·관협력체 'K-사이버보안 대연합' 출범
  - 신속한 위협정보 공유에 중점을 두고 8개 유관 협·단체 및 1만9,000곳 회원사가 참여

- **한국은 사이버보안 관련 기본법 부재, 체계적이고 효율적 대응을 위한 법적 근거 마련 시급**
  - 주요국이 법률 제정을 토대로 정부 정책과 제도를 뒷받침하고 있는 데 반해, 한국은 사이버보안 관련 기본법이 부재한 상황
  - 최초의 사이버보안 관련 규정은 1986년에 제정된 '전산망 보급 확장과 이용촉진에 관한 법률'이나, 사이버보안에 대한 인식 부재로 실효성 미흡

- 정보통신기술의 발달과 정보화에 대한 수요 증가로 정보통신 관련 법률이 다수 제정* 되어 사이버 안전 관련 규정 산재해 있으나, 사이버공격 대응에는 역부족

  * '정보통신망 이용촉진 및 정보보호 등에 관한 법률('20)', '개인정보보호법('20)', '정보통신기반보호법('19)', '통신비밀보호법('20)', '정보보호산업의 진흥에 관한 법률('18)', '국가정보화기본법('19)', '전자정부법('17)', '전자금융거래법('17)' 등이 사이버보안 관련 법률

- 공공부문의 정보보호 추진체계 규정 등 국내 사이버보안에서 중요한 역할을 하는 '국가사이버 안전관리 규정'은 대통령 훈령에 불과한 실정

- 한국은 사이버보안 관련 법제 정비가 시급하나, 현재 국회에 계류 중인 사이버보안법은 국가 정책집행력 강화와 개인정보침해에 대한 견해 차이로 인해 처리가 지연되고 있음

- 한국이 국가차원의 범정부 사이버보안 정책을 수립한 것은 2016년으로 주요국 대비 늦은 편이나, 정보보호기술개발 및 육성에 관한 정책은 꾸준히 진행
- 최근 사이버보안을 국가필수전략기술로 선정하고 관련 투자를 확대
- 정책에 민·관협력 체계를 반영하고 규제 완화를 통해 민간투자를 유도
- 국내 사이버보안 정책은 부처별 활용하는 용어가 상이하고, 분야별 보안체계 및 실행 조직이 분산되어 있어 정책 및 대응체계 정비 필요
- 사이버보안 기본법률이 부재한 상황, 사이버보안기본법 제정 및 산재해 있는 사이버보안 관련 규정 정비 시급

3 국내 사이버보안 분야 정부 R&D 투자 현황

가. 정부 R&D 예산 중 사이버보안 R&D 투자 현황

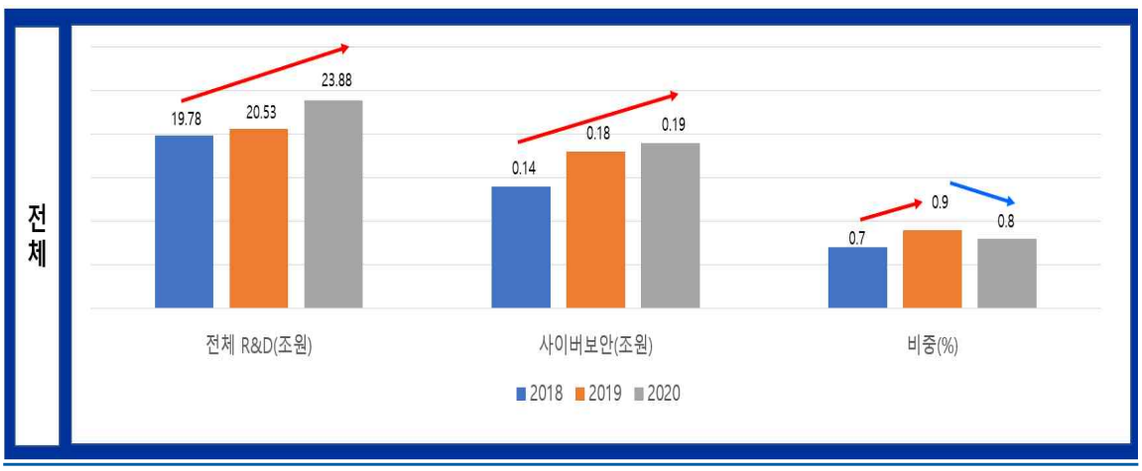
- **우리나라 전체 R&D 예산 중 사이버보안 분야 투자**
  - 연도별 추이를 살펴보면, 사이버보안 분야의 정부 R&D 예산은 지속적으로 증가하고 있으나, 전체 정부 R&D 내에서 차지하는 투자 비중은 '19년 이후 하락하는 추세

표 2-8 정부 R&D 중 사이버보안 투자 현황

	2018년	2019년	2020년
전체 R&D 예산(조원)	19.78	20.53	23.88
사이버보안 예산(조원)	0.14	0.18	0.19
비중(%)	0.7	0.9	0.8

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-1 정부 R&D 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

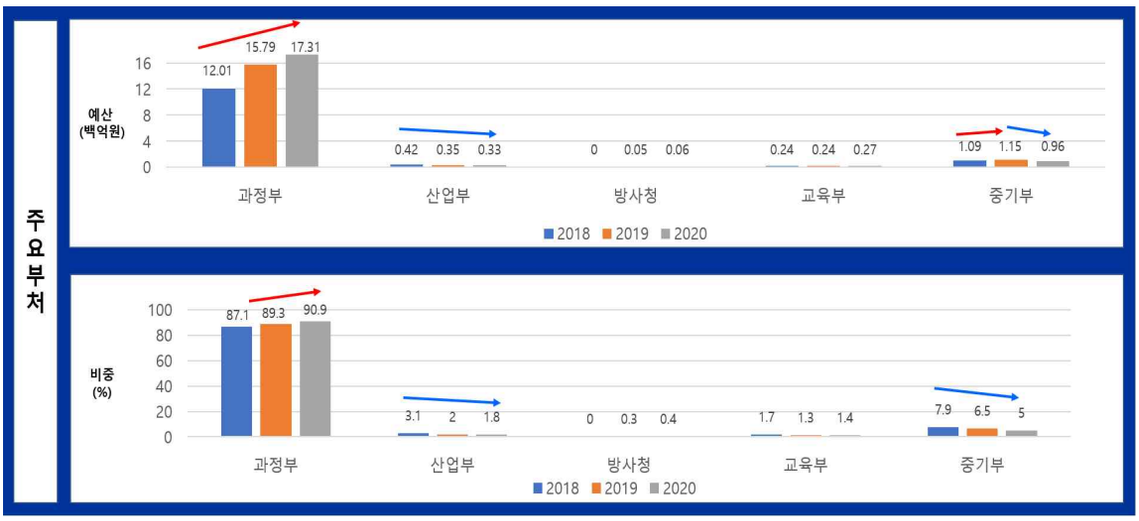
- **주요부처별 정부 R&D 예산 중 사이버보안 포트폴리오 동향**
  - '20년 기준 과기정통부는 17.31조원으로(전체 90.9%) 가장 많은 예산을 지출
  - 연도별 추이를 살펴보면, 과기정통부의 사이버보안 관련 예산과 비중 모두 증가하고 있는 반면, 산업부는 예산과 비중 모두 지속적으로 하락하고 있으며, 중기부는 '19년 이후 예산과 비중 모두 하락

표 2-9 주요부처별 R&D 예산 중 사이버보안 투자 현황

부처	2018년			2019년			2020년		
	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)
과정부	12.01	154	87.1	15.79	183	89.3	17.31	211	90.9
산업부	0.42	14	3.1	0.35	15	2	0.34	13	1.8
방사청	0	0	0	0.05	1	0.3	0.06	1	0.4
교육부	0.24	58	1.7	0.24	60	1.3	0.27	52	1.4
중기부	1.09	94	7.9	1.15	100	6.5	0.96	75	5

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-2 주요부처별 R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

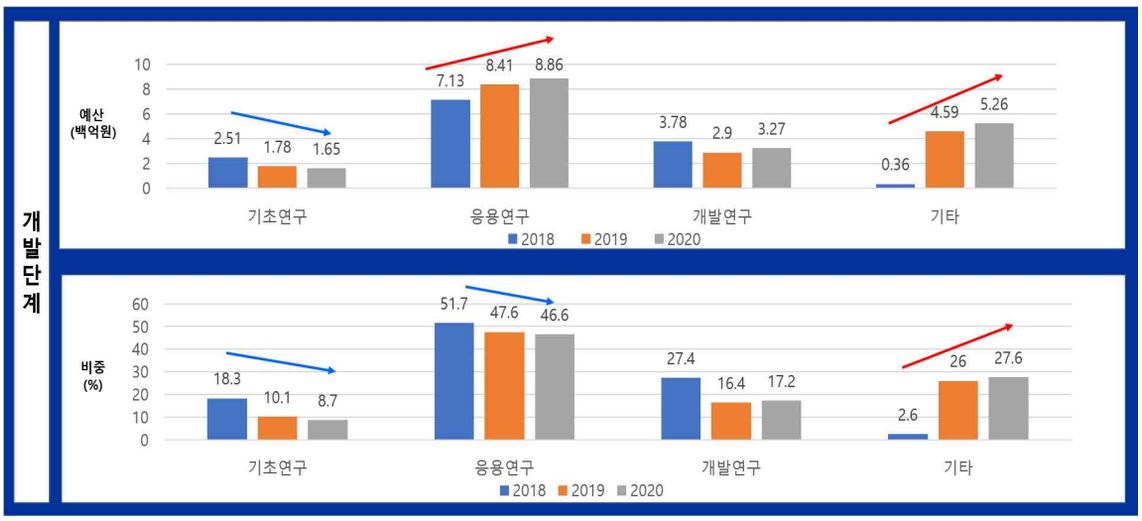
- **개발단계별 정부 R&D 예산 중 사이버보안 포트폴리오 동향**
  - '20년 기준 응용연구 단계에서 가장 많은 비중(46.6%)을 차지하고 있으며, 기초연구 단계가 가장 낮은 비중(8.7%)으로 나타남
  - 연도별 추이를 살펴보면, 응용연구 단계는 예산은 증가하고 있으나 비중은 하락, 기초연구 단계는 예산과 비중 모두 하락, 특히 비중이 큰폭으로 하락

표 2-10 개발단계별 정부 R&D 예산 중 사이버보안 투자 현황

연구개발단계	2018년			2019년			2020년		
	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)
기초연구	2.51	135	18.3	1.78	158	10.1	1.65	150	8.7
응용연구	7.13	36	51.7	8.41	54	47.6	8.86	67	46.6
개발연구	3.78	143	27.4	2.90	146	16.4	3.27	129	17.2
기타	0.36	9	2.6	4.59	10	26	5.26	15	27.6

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-3 개발단계별 정부 R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

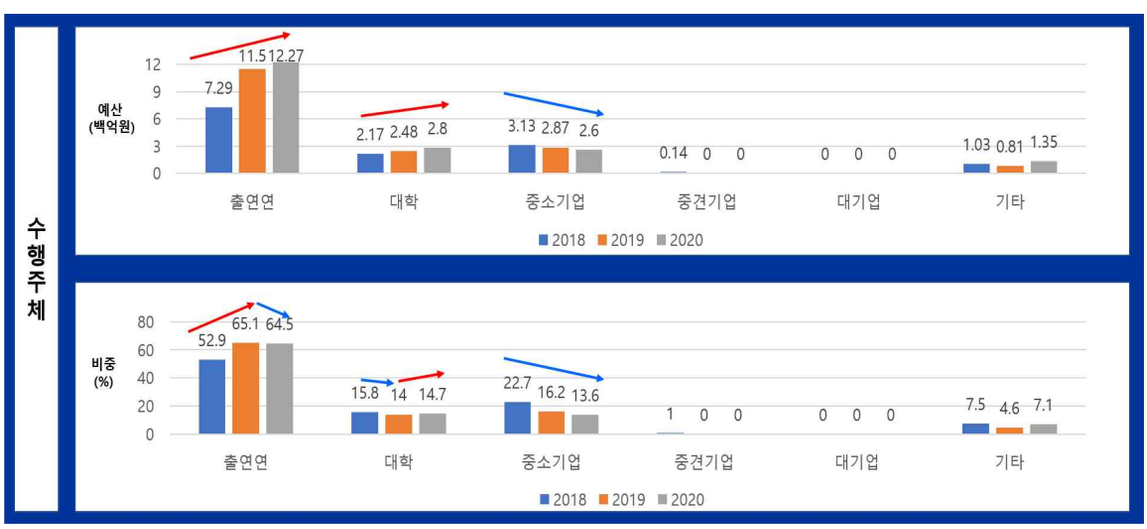
- **수행주체별 정부 R&D 예산 중 사이버보안 포트폴리오 동향**
  - '20년 기준 출연(연)이 64.5%로 가장 높은 비중을 차지하고 있으며, 다음으로 대학, 중소기업 순으로 높은 점유율을 기록
  - 연도별 추이를 살펴보면, 출연(연)의 예산이 매해 증가하는 것과 비교하여, 비중은 '19년을 기준으로 하락
  - 대학의 예산이 꾸준히 증가하는 것과 반대로, 중소기업은 예산과 비중 모두 하락

표 2-11 수행주체별 정부 R&D 예산 중 사이버보안 투자 현황

수행주체	2018년			2019년			2020년		
	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)
출연연	7.29	23	52.9	11.5	31	65.1	12.27	31	64.5
대학	2.17	149	15.8	2.48	186	14	2.80	191	14.7
중소기업	3.13	138	22.7	2.87	143	16.2	2.60	128	13.6
중견기업	0.14	1	1	0	0	0	0	0	0
대기업	0	0	0	0	0	0	0	0	0
기타	1.05	12	7.6	0.82	8	4.7	1.36	11	7.1

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-4 수행주체별 정부 R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

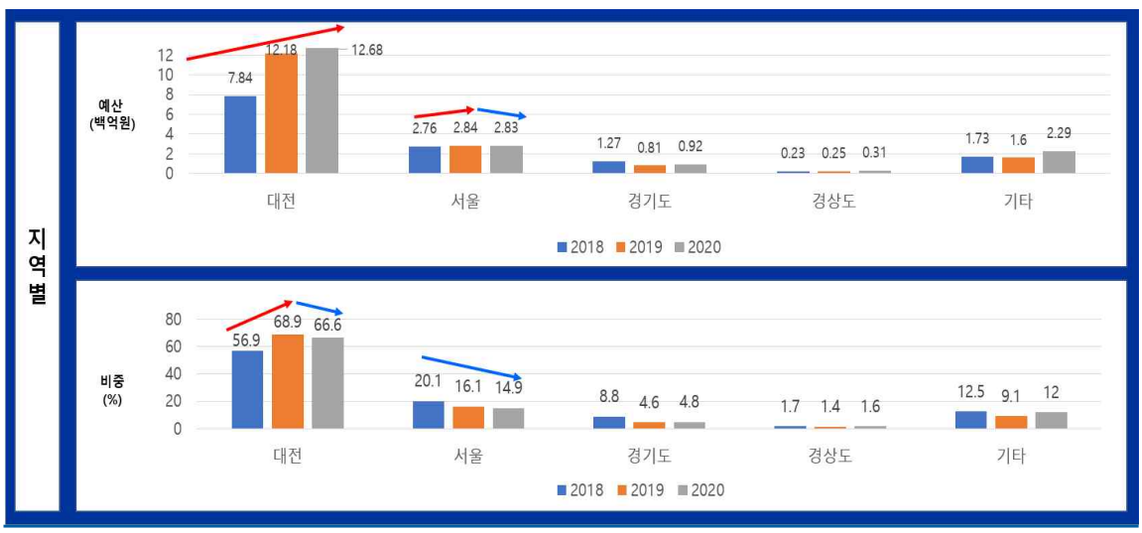
- **지역별 정부 R&D 예산 중 사이버보안 포트폴리오 동향**
  - '20년 기준 대전은 전체 66.6%로 가장 높은 비중을 차지, 다음으로 서울, 경기도 순으로 높은 비중을 나타냄
  - 연도별 추이를 살펴보면, 대전은 예산이 꾸준히 증가하는 것과 비교하여 비중은 '19년 이후 하락, 서울도 비중에서 큰 폭으로 하락

표 2-12 지역별 정부 R&D 예산 중 사이버보안 투자 현황

지역	2018년			2019년			2020년		
	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)
대전	7.84	48	56.9	12.18	58	68.9	12.68	54	66.6
서울	2.76	129	20.1	2.84	154	16.1	2.83	6	14.9
경기도	1.27	55	8.8	0.81	61	4.6	0.92	63	4.8
경상도	0.23	17	1.7	0.25	15	1.4	0.31	14	1.6
기타	1.73	74	12.5	1.60	80	9.1	2.29	86	12

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-5 지역별 정부 R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

나. 정부 ICT R&D 예산 중 사이버보안 분야 투자 동향

- **우리나라 ICT R&D 예산 현황**
  - 정부 ICT R&D 예산은 연평균 13.6% 성장으로, 정부 전체 R&D 예산의 성장률(9.9%)와 비교하여 급성장
  - 우리나라 ICT R&D 예산은 매해 꾸준히 증가, 특히 '20년 기준 전체 R&D 예산에서 ICT R&D 예산이 차지하는 비중이 급격하게 증가

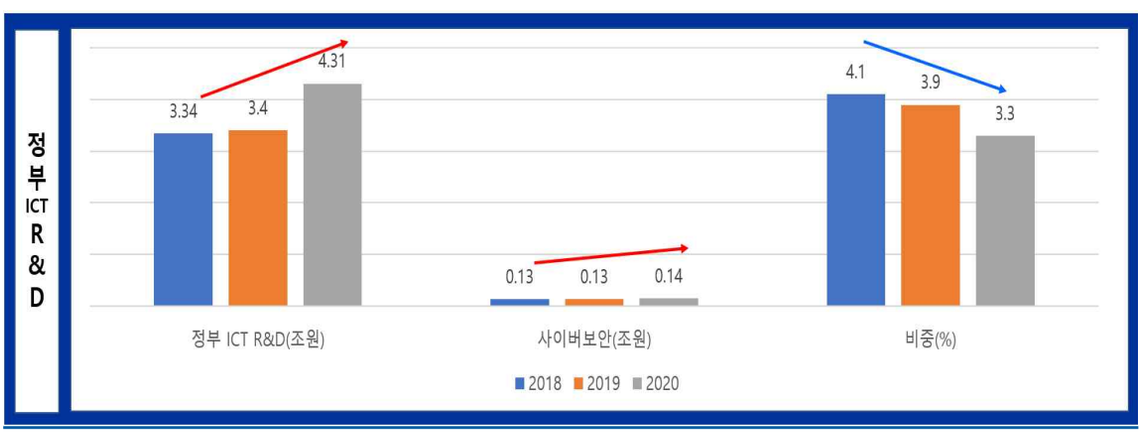
- **ICT R&D 예산 중 사이버보안 포트폴리오 동향**
  - 정부의 ICT R&D 예산액은 매해 크게 증가한 반면, 사이버보안에 예산은 큰 성장이 나타나지 않음
  - 정부 ICT R&D에서 사이버보안이 차지하는 비중이 매해 하락하고 있으며, 그 하락폭도 증가 추세

표 2-13 정부 ICT R&D 예산 중 사이버보안 투자 현황

	2018년 예산(조원)	2019년 예산(조원)	2020년 예산(조원)
정부ICT투자	3.34	3.40	4.31
사이버보안	0.13	0.13	0.14
비중(%)	4.1	3.9	3.3

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-6 정부 ICT R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

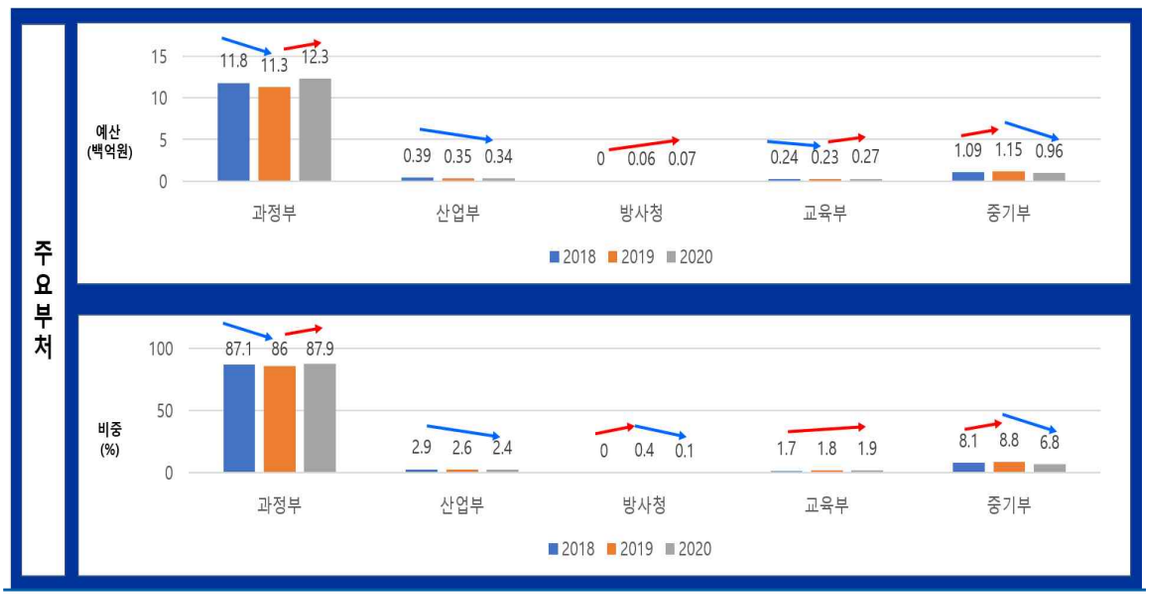
- **각 주요 부처별 정부 ICT R&D 예산 중 사이버보안 포트폴리오 동향**
  - '20년 기준 과기정통부가 가장 많은 비중을 차지하는 부처로, 사이버보안 관련 전체 ICT R&D 예산 중, 87.9%를 집행
  - 두 번째로 중기부가 높은 비중을 차지하고 있으나, '20년에 비중이 하락
  - 연도별 추이를 살펴보면, 산업부는 예산과 비중 모두 하락하고 있으며, 중기부는 '19년 이후부터 예산과 비중 모두 하락

표 2-14 주요부처별 정부 ICT R&D 예산 중 사이버보안 투자 현황

부처	2018년			2019년			2020년		
	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)
과정부	11.8	152	87.1	11.3	179	86	12.3	208	87.9
산업부	0.39	13	2.9	0.35	15	2.6	0.34	13	2.4
방사청	0	0	0	0.06	1	0.4	0.07	1	0.1
교육부	0.24	58	1.7	0.23	60	1.8	0.27	52	1.9
중기부	1.09	94	8.1	1.15	100	8.8	0.96	75	6.8

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-7 주요부처별 정부 ICT R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

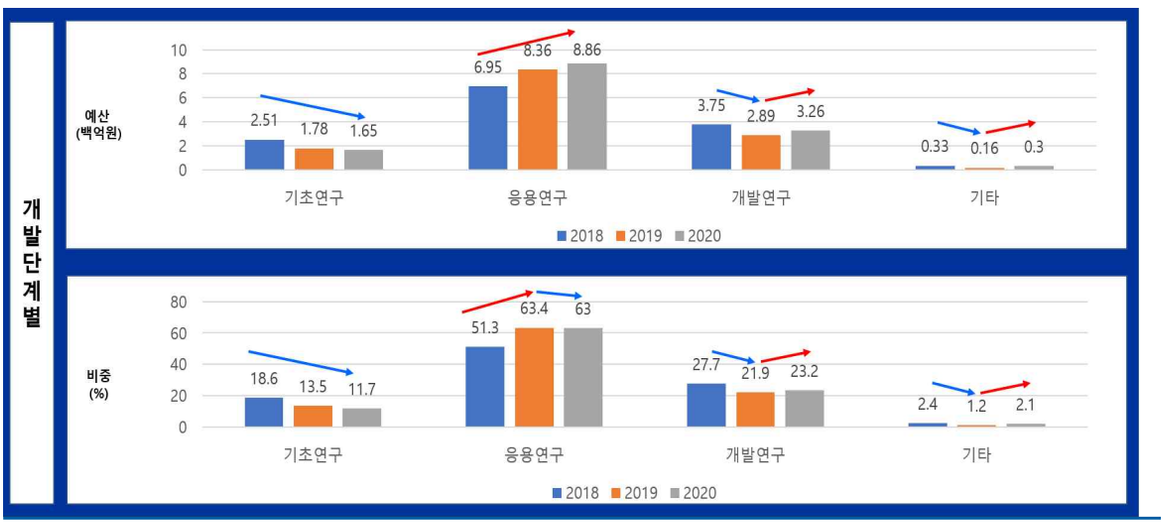
- **개발단계별 정부 ICT R&D 예산 중 사이버보안 포트폴리오 동향**
  - '20년 기준 개발단계에서는 응용연구가 가장 많은 예산인 8.86백억원(전체 63%)이 집행되었으며, 반대로 기초연구는 1.65백억원(11.7%)으로, 가장 적은 예산이 할당
  - 연도별 추이를 살펴보면, 응용연구는 예산이 꾸준히 증가하는 반면, 기초연구는 예산과 비중 모두 하락

표 2-15 개발단계별 정부 ICT R&D 예산 중 사이버보안 투자 현황

연구개발단계	2018년			2019년			2020년		
	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)
기초연구	2.51	135	18.6	1.78	158	13.5	1.65	150	11.7
응용연구	6.95	35	51.3	8.36	52	63.4	8.86	66	63
개발연구	3.75	142	27.7	2.89	145	21.9	3.26	128	23.2
기타	0.33	8	2.4	0.16	6	1.2	0.30	11	2.1

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-8 개발단계별 정부 ICT R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

- **수행주체별 정부 ICT R&D 예산 중 사이버보안 포트폴리오 동향**

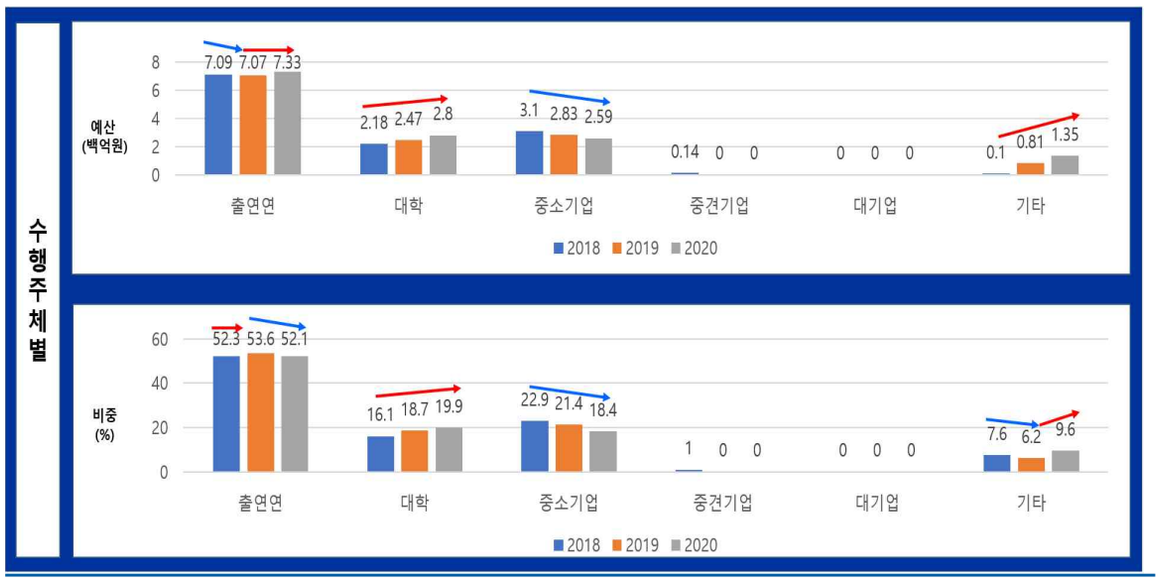
  - '20년 기준 출연(연)의 비중이 가장 높은 52.1%를 차지하고 있으며, 대학은 19.9%로 두 번째로 높은 비중을 차지함
  - 연도별 추이를 살펴보면, 출연(연)은 '19년을 기준으로 예산이 상승하고 있는 반면, 비중은 하락
  - 중소기업은 예산과 비중이 모두 하락하고 있는 반면, 대학은 비중과 예산 모두 상승

표 2-16 수행주체별 정부 ICT R&D 예산 중 사이버보안 투자 현황

수행주체	2018년			2019년			2020년		
	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)
출연연	7.09	21	52.3	7.07	28	53.6	7.33	28	52.1
대학	2.18	149	16.1	2.47	184	18.7	2.80	190	19.9
중소기업	3.10	137	22.9	2.83	141	21.4	2.59	127	18.4
중견기업	0.14	1	1.0	0	0	0	0	0	0
대기업	0	0	0	0	0	0	0	0	0
기타	0.1	10	7.6	0.81	7	6.2	1.35	10	9.6

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-9 수행주체별 정부 ICT R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

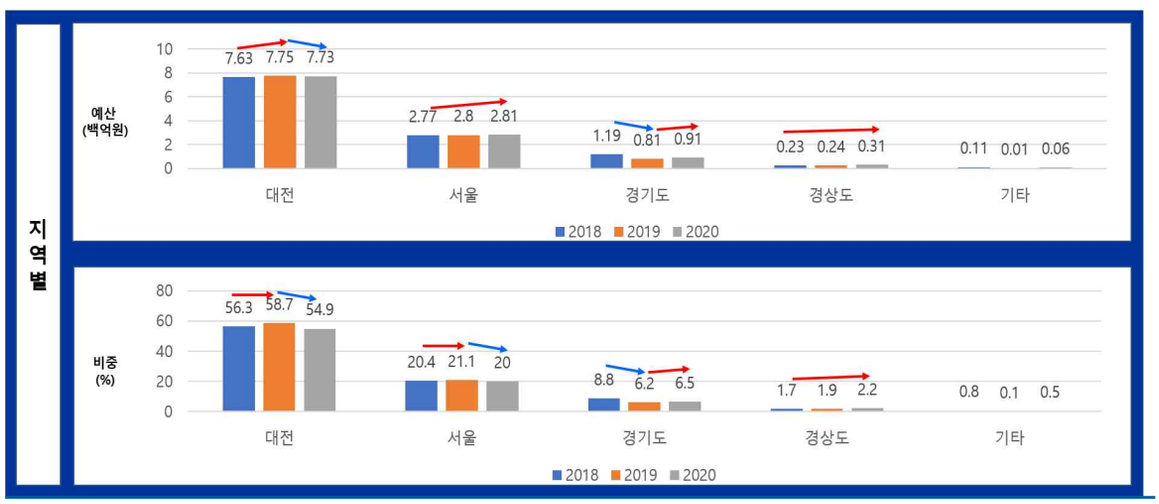
- **지역별 정부 ICT R&D 예산 중 사이버보안 포트폴리오 동향**
  - '20년 기준 대전은 전체 지역의 54.9%를 차지하여 가장 높은 지역이며, 다음으로는 서울 및 경기 지역이 높은 비중으로 할당
  - 연도별 추이를 살펴보면 대전은 '19년을 기준으로 예산과 비중 모두 하락한 반면, 경기도는 예산과 비중 모두 상승, 경상도는 매년 예산과 비중 모두 꾸준히 증가

표 2-17 지역별 정부 ICT R&D 예산 중 사이버보안 투자 현황

지역	2018년			2019년			2020년		
	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)	예산(백억원)	과제수(수)	비중(%)
대전	7.63	46	56.3	7.75	55	58.7	7.73	51	54.9
서울	2.77	129	20.4	2.80	151	21.1	2.81	142	20
경기도	1.19	54	8.8	0.81	61	6.2	0.91	62	6.5
경상도	0.23	17	1.7	0.24	14	1.9	0.31	14	2.2
기타	0.11	2	0.8	0.01	1	0.1	0.06	3	0.5

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-10 지역별 정부 ICT R&D 예산 중 사이버보안 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

다. 혁신본부 ICT융합전문위원회 R&D 투자 중 사이버보안 포트폴리오 동향

- **ICT융합전문위원회 R&D 예산 현황**
  - ICT융합전문위원회 R&D 예산은 '18년 1.73조원, '19년 1.87조원, '20년 2.26조원으로 연평균 14.2% 성장하여, 전체 R&D 예산 성장률(9.5%) 보다 높음

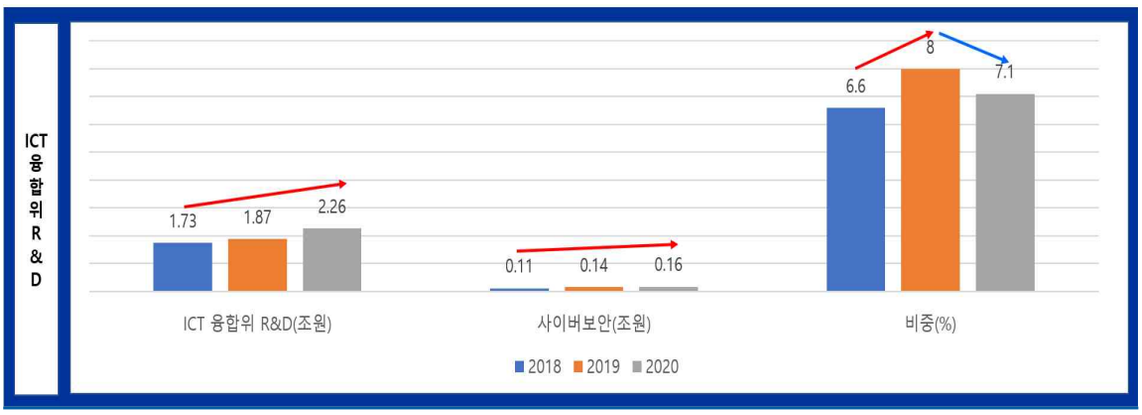
- **ICT융합전문위원회 R&D 예산 중 사이버보안 포트폴리오 현황**
  - ICT융합전문위원회 전체 예산과 사이버보안 예산은 꾸준히 증가하는 반면, 사이버보안 분야의 투자 비중은 '19년 이후 하락 추세

표 2-18 ICT융합전문위원회 R&D 예산 중 사이버보안 분야 투자 현황

	2018년 예산(조원)	2019년 예산(조원)	2020년 예산(조원)
ICT 융합위 R&D 전체	1.73	1.87	2.26
ICT 융합 중 사이버보안	0.11	0.14	0.16
비중(%)	6.6	8	7.1

※ 출처: NTIS 사업과제 DB 기반으로 구성

그림 2-11 ICT융합전문위원회 R&D 예산 중 사이버보안 분야 투자 추이



※ 출처: NTIS 사업과제 DB 기반으로 구성

- R&D 예산 현황을 살펴본 결과, 사이버보안 예산은 매해 증가하는 반면 비중은 '19년 이후 감소

III 사이버보안 기술 동향 및 전망

1 사이버보안 분야 중점기술

- 미래 사이버 안전과 기술경쟁력 확보에 필수적인 중점기술 분야를 다음의 〈표 3-1〉과 같이 선정

표 3-1 사이버보안 중점기술 및 세부 요소기술

중분류 기술	정 의	세부 요소기술
데이터 활용 보안	데이터 활용 전주기에 걸쳐 프라이버시 및 데이터 주권 보호 중심으로 데이터 활용성을 강화하기 위한 기술	• 고비도 암호 설계, 암호키 관리 및 검증기술 • 프라이버시 강화 컴퓨팅 기술 • 양자내성암호 분석 및 전환 기술 • 암호화 기반 데이터 검색/활용기술(동형암호 등) • 비식별화/익명화 기술, 데이터 주권강화기술
차세대 네트워크 보안	5G+ 융합서비스 및 미래 6G 네트워크 환경에서 보안위협을 대응하기 위한 지능형 사이버보안 기술	• 5G/5G+ 융합서비스 보안위협 대응 기술 • 사설 5G/특화망 네트워크 보안 기술 • 6G 네트워크 보안 내재화 기술 • 인공지능 기반 지능형 보안관제 기술 • 인공지능 기반 사이버공격 시뮬레이션 기술
시스템 · 디바이스 보안	대규모 IoT 디바이스를 포함한 다양한 ICT 기기의 안전한 사용을 위한 시스템·디바이스 보안 기술	• 시스템/디바이스 취약점 진단 자동화 • HW/SW 공급망 보안 기술 • AI기반 악성코드 분석 기술 • 지능형 IoT 디바이스 보안 기술
신 디지털 플랫폼 보안	Web 3.0, 메타버스 등 신 디지털 플랫폼 및 가상융합경제의 이용자 보호 기술	• 분산 디지털 신원관리 기술 • 메타버스 보안 기술 • 탈중앙화 가상경제 보안 기술 • 비대면 보안 기술
사이버 범죄 대응	다크웹, 랜섬웨어 등 사이버범죄 근원지 추적 및 디지털 포렌식 관련 기술	• 스마트기기 디지털 포렌식 기술 • 다크웹 사이버 범죄 근원지 추적 기술 • 랜섬웨어 공격 근원지 추적 및 피해복구 기술
융합 산업 보안	SoC 디지털 가속화에 따른 주요 기반 시설 및 국방 분야에 적용 가능한 IT와 OT의 융합보안 기술	• 국방 보안 기술(통신, 무기체계, 백신 등) • IT+OT 융합보안 기술 (해양·선박 등) • 저궤도 위성 통신 인프라 보안 기술
물리 환경 안전·보안	CCTV 등 영상보안시스템이 자율적으로 위협을 인식, 예측, 협업·대응하고 보안 역기능을 원천적으로 방지하는 개방형 영상보안 AI 기술	• 온-디바이스 초지능 CCTV 기술 • 개방형 영상보안플랫폼 기술 • 공공/민간 영상보안플랫폼 자율보호 기술

2 국내·외 사이버보안 기술개발 동향

가. 데이터 활용 보안

- (국외) 데이터경제 시대 주도권 확보를 위한 데이터 활용 기반 플랫폼 구축 경쟁이 가속화되며, 주요 선진국 중심으로 **개인의 데이터 주권 보호를 위한 핵심 기술** 개발 중
  - **(데이터 주권 보호 강화)** GDPR로 대표되는 개인 데이터에 개인의 권리 보호를 위한 정책적 움직임 활발
    - ※ EU는 GDPR 제정을 통해 데이터에 대한 개인의 권리를 보장하고, 기업이 개인 데이터를 수집·활용하는 과정에 대한 개인 정보 보호 기준을 마련
    - ※ (미)캘리포니아 주는 GDPR에 대응되는 CCPA(California Consumer Privacy Act)를 2020년 7월 시행, 타 주에서도 관련 법 제정 논의가 활발히 진행
  - **(동형암호)** 암호화된 데이터 활용이 가능한 동형암호 기술에 대한 관심이 여전히 높으며, 원천기술 개발 위주의 연구를 벗어나 단점(느린 연산속도, 큰 암호문 등)을 보완하기 위한 상용화 연구가 활발히 진행
    - ※ 미국(DARPA)는 DPRIVE(Data Protection in Virtual Environments) 프로젝트를 통해 동형암호 실용화를 위한 하드웨어 및 소프트웨어 연산 가속화 기술 연구를 진행 중 ('20.3)
    - ※ Microsoft Edge 브라우저에 동형암호기술을 적용, 사용자의 비밀 번호가 유출되었는지 확인하고 경고하는 password monitor 서비스 제공 ('21)
  - **(데이터 신뢰·유통 플랫폼)** 데이터에 대한 주권 보장을 기반으로 데이터를 다양한 산업에 활용하기 위한 데이터 유통 플랫폼 기술 개발이 진행
    - ※ 일본은 데이터 산업 활성화를 위한 데이터 신탁형 모델인 데이터 뱅크 사업 추진
    - ※ 독일 프라운호퍼 주도의 유럽 산업 연합체인 IDS(industrial data space)는 산업 도메인간 안전한 데이터 교환에 관한 연구 수행 중
  - **(양자내성암호)** 양자 컴퓨터 현실화에 따른 암호 안전성 보장을 위해, 미국 NIST를 중심으로 양자내성암호 도입을 위한 기반 마련
    - ※ 미국 NIST에서는 2021년 7월에 3라운드 PQC 컨퍼런스를 개최하였고, 이어지는 보안성 평가 등을 통해 2024년 제정을 목표로 하고 있음
- (국내) 데이터 산업 활성화 추진을 위해 데이터가 생성, 저장, 갱신, 활용, 폐기되는 전주기에서 **데이터에 대한 개인의 자기 결정권 및 신뢰 유통을 보장하기 위한 기반** 마련
  - **(데이터 주권 보호 강화)** 데이터 산업 활성화를 위한 제도적·정책적 기반 마련 중
    - ※ 데이터 3법 개정으로 안전한 데이터 활용 기반을 마련하고, 데이터 유통·산업육성을 위한 데이터 기본법 등 디지털 전환 3법 추진 중

※ 디지털 뉴딜 일환인 데이터 댐 구축을 통해 데이터 수집·유통·활용에 이르는 데이터 가치사슬 전 주기에서 데이터 활용 활성화 추진

- **(동형암호)** 동형암호 원천 기술에 대한 국제적 경쟁력을 확보하고 있으며, 동형암호 상용화를 위한 다양한 연구를 진행 중

※ 서울대학교는 자체계발한 동형암호 알고리즘 CKKS를 기반으로 세계 최고 수준의 동형암호 라이브러리 HEaaN을 구현하여 국제적 경쟁력 확보

※ ETRI는 동형암호 상용화를 위한 HW지원 동형암호 가속 처리 기술을 개발 중이며, 통계청은 동형암호 기반 국가 통계분석시스템 개발을 진행 중 ('21~)

- **(데이터 신뢰·유통 플랫폼)** 암호화를 통한 데이터 프라이버시 보호를 기반으로 데이터 산업 전영역에 대한 데이터 유통 보호를 위한 연구가 진행 중

※ 개인정보의 자기 결정권 강화를 위한 분산환경 중심의 효율적인 데이터 수집/저장/열람/전달 기술 개발

※ 세계적인 데이터 유통 플랫폼 구축 경쟁에 대응하여, 데이터 주권 보호 기술 확보 추진, 참여자들 자율에 따른 데이터 가치산정 및 분배/거래 기술 진행

- **(양자내성암호)** 국제적 양자내성암호 도입 움직임에 대응하기 위한 연구가 대학, 출연연을 중심으로 진행 중

※ 양자컴퓨터에 취약한 기존 암호 체계를 양자내성암호 체계로 단계적 전환을 위하여 LGU+는 양자내성암호를 자사 통신채널에 선도적으로 적용하는 시범사업 추진 ('21)

※ ETRI는 고전 암호와 양자내성암호에 대한 양자컴퓨터 공격을 고려한 양자안전성 분석 연구 진행 중

※ 국보연은 국산 양자내성암호 개발을 위한 KpqC 연구단을 발족하여 국내 연구진 중심의 공모전 추진('21~)

나. 차세대 네트워크 보안

- (국외) 5G/6G 및 네트워크보안 관제 분야에서 **인공지능 기술을 활용한 선도형 기술 개발**에 집중
  - **(5G/5G+ 융합서비스 보안위협 대응 기술)** 글로벌 기술 패권 경쟁 심화에 따라 3GPP 표준화 및 AI 보안 등 선도형 기술 개발 중
  - **(사설 5G/특화망 네트워크 보안 기술)** 3GPP와 5G-ACIA를 중심으로 사설 5G 구축 유형별 보안 기술 개발 및 표준화 추진 중
  - **(6G 네트워크 보안 내재화 기술) 6G 플래그쉽 연구**를 수행 중인 핀란드 오울루대학은 6G 네트워크 환경에서 **AI 기반 보안 기능과 신뢰망 구조를 연구** 중

※ 해외 주요국에서는 6G 원천기술 확보 및 기술 표준화 선점을 위한 6G R&D를 진행하고 있으며, 보안 관련한 주요 연구 이슈와 아이템을 도출하고 있는 초기 단계임

  - **(인공지능 기반 지능형 보안관제 기술)** 기존 SIEM(보안 정보 및 이벤트 관리)에 보안 오케스트레이션, 자동화, 대응 기능에 위협 인텔리전스 관리 기능 개발 본격화

- **(인공지능 기반 사이버공격 시뮬레이션 기술)** Pen-test, Cyber Range 등의 분야에서 선제적으로 인공지능 활용한 사례가 있으나, 공격 시나리오 위주 시뮬레이션 도구가 대부분

※ 가트너에서는 Autonomous Penetration Test and Red Teaming을 이머징 서비스 도메인으로 새롭게 추가 (21)

- (국내) 5G+ 핵심서비스 등 국내 환경에 맞게 기술 개발이 진행되고 있으나, 미래 네트워크 보안기술에 대한 대응이 다소 미흡
  - **(5G/5G+ 융합서비스 보안위협 대응 기술)** 5G+ 핵심서비스를 위한 클라우드, 5G 엣지망·MEC 등 4차 산업혁명 핵심 인프라에 대한 보안 기술개발 추진

※ 5G+ 핵심서비스의 안전한 이용환경 보장을 위한 5G 엣지망·MEC·코어망 보안위협 및 이상행위 탐지·대응, 핵심서비스별 보안모델 개발 등

  - **(사설 5G/특화망 네트워크 보안 기술)** 정부의 5G 특화망(이음 5G) 도입 추진에 따라 초기 단계인 사설 5G/특화망 보안 기술 개발이 본격화될 전망

※ 과학기술정보통신부, '5G 특화망 정책방안', 2021.1.26

  - **(6G 네트워크 보안 내재화 기술)** 6G 신규 기술과 서비스 모델을 분석하고 있으나, 6G 네트워크 공격 모델 및 **보안 내재화 기술에 대한 선도적 연구는 전무**

※ 6G 기술은 '28~'30년경에 상용화될 것으로 예상되므로, 全산업 영역에 6G 기반의 융합 서비스가 안정적으로 적용·고도화되기 위한 기반 기술 연구 착수('20년 미래 이동통신 R&D 추진전략, 과기부)

  - **(인공지능 기반 지능형 보안관제 기술)** 사이버 공격 대응에 인공지능 기술이 적용되어 있으며, 신종 보안위협에 대한 탐지 정확성을 높이기 위해 인공지능 기술 활용 중

※ 국가정보자원관리원(NIRS)은 AI 기반 적응형 보안체계 사업 2018년부터 3개년 일정으로 추진 전자정부서비스를 비롯한 각종 공공 서비스 인프라를 대상으로 인공지능 보안 플랫폼 구축

  - **(인공지능 기반 사이버공격 시뮬레이션 기술)** 인공지능을 활용한 사이버공격 시뮬레이션 기술보다는 대부분 공격도구 자동화 수준에 그치고 있음

다. 시스템 · 디바이스 보안

- (국외) **인공지능을 활용한 보안 위협 탐지 성능향상**에서 성과를 보이고 있으며, **국가적 차원의 공급망 위협대응 추진**
  - **(AI기반 악성코드 분석 기술)** 글로벌 보안기업들은 AI를 활용한 변종 악성코드 탐지 기술을 연구하고 있으며, **머신러닝 기반의 악성코드 분석 솔루션을 출시** 중

※ 미국 Invincea, Crowd Strike, Kaspersky Lab 등은 머신러닝 기술을 활용한 안티바이러스 솔루션을 제공하며 높은 악성코드 탐지율을 제공하나, 오탐율 또한 높아 보완이 필요함

  - **(지능형 IoT 디바이스 보안 기술)** 새로운 보안 위협에 노출되는 IoT 디바이스를 인지하고 능동적으로 차단하는 위협헌팅기반 보안 통제 기술에 대한 연구 진행 중

※ VIDDER 'PrecisionAccess' 과 같이 IoT 디바이스의 추가 인증를 통해 네트워크 접속이 가능한 제품들이 있으나 주로 클라우드 기반 기술로 임베디드 기기 등에 적용하기에 미흡

- **(HW/SW 공급망 보안)** 미국, 유럽, 일본 등은 국가주도로 공급망 위협 대응 기술개발을 추진하고 있으며, IC칩 수준의 악성회로 분석/탐지 기술은 한국과 높은 기술 격차가 존재

※ 미국은 국가안보차원에서 NIST 중심으로 관련 프로세스/도구/관련문서를 공개하고 있으며, 중국은 타 국가 공급망 공격(예:2018년 Supermicro사건) 의혹을 가질 정도의 기술력 확보가 예측됨

● (국내) **인공지능을 활용하는 보안 연구가 본격적으로 진행**되고 있으며, SW 중심에서 **HW 공급망 보안 연구가 본격적으로 추진** 중

- **(AI기반 악성코드 분석 기술)** 기하급수적으로 증가하는 악성코드에 대응하기 위해 **AI 기술을 도입하여 자동 대응**할 수 있는 악성코드 분석 기술 연구 진행 중

※ 안랩은 ASD(AhnLab Smart Defense) 인프라에서 수집한 약 2,300만개의 실행파일을 자체적으로 개발한 머신러닝 시스템으로 약 70%정도의 분류 정확도를 제시하고 있음

- **(지능형 IoT 디바이스 보안 기술)** 서비스 Context변화에 능동적으로 적용하고 개별적으로 관리 차단하는 보안 통제 기술에 대한 연구가 필요

※ 보안위협에 대한 시각화나 보안위협 인지 기술에 인공지능을 적용한 제품으로 시큐레이어의 'eyeCloudSiM' 이 있으나, 대량 단순 반복 업무를 빠르게 수행하는 수준임

- **(HW/SW 공급망 보안)** 국내는 SW 공급망 위협에 중심으로 연구되어 왔으나, 최근에는 ETRI를 중심으로 하드웨어 수준의 보안 취약점 조사·검증 원천기술 연구 개발 중

※ 외산 디지털 장비에 대한 높은 의존 상태를 고려하여, 해당 장비들에 대한 분석 기술/장비/인력의 확보를 통한 안전성 검증 자립도를 높일 필요가 있음

라. 신 디지털 플랫폼 보안

● (국외) 급증하는 메타버스, NFT 등 **신 디지털 서비스로 파생되는 부작용(아바타 아이디 도용, 디지털 자산 복제·위조, 디지털 성범죄 등) 확대로 보안 선도 기술 확보 경쟁**

- **(분산 디지털 신원관리)** 마이크로소프트, 화웨이, 쇼카드, 유포트 등은 **DID(분산 신원증명) 솔루션을 개발하여 공공·민간 영역의 사용자 신원증명 서비스에 활용** 중

※ 마이크로소프트는 2021년 3월말 비트코인 블록체인 기반 분산신원증명(DID) 기술인 아이온 발표

- **(메타버스 보안) 현실-가상 공간의 새로운 보안 기술과 프라이버시 보호 기술에 대한 필요성 증가** 추세

※ 현재의 메타버스는 사이버세계만을 다루는 초기 단계로 기존 보안기술을 활용하는 수준이나 현실과 가상이 혼합 연결되는 근미래 메타버스는 사용자의 경제, 문화, 사회 활동 공간으로 확대되어 보호대상 증가

- **(탈중앙화 가상경제 보안)** 오픈씨(OpenSea), 디센트럴랜드(Decentraland) 등을 개발·운영 중이나 **해킹사고와 복제·위조 등 문제로 대응 기술 수요 증가**

※ 대체불가토큰(NFT) 시장의 주요 마켓플레이스인 오픈씨는 '22년 1월 하루 최고 거래액 2억6100만달러 기록하고 있으나 '22년 1월과 2월 두차례의 해킹 공격으로 피해 발생으로 거래량 감소

- **(비대면 보안) 비대면 사용자 인증, 제로 트러스트 보안, 사이버보안 메시 등의 연구**가 마이크로소프트, IBM, 시스코 등 글로벌 기업에서 활발히 진행되어 보안 솔루션 출시

※ 2023년까지 전체 기업의 60%가 사설가설망(VPN)에서 벗어나 제로 트러스트(Zero Trust) 기반으로 보안 개념을 바꿀 전망('20, Gartner)

※ 제로트러스트 보안은 내·외부의 경계 없이 민감한 데이터·서비스를 활용할 수 있도록 이용자, 장치에 대한 신뢰도를 통합 검증하는 기술

※ 사이버보안 메시는 사람이나 신원을 중심으로 보안 경계를 정의하여 독립된 환경과 분산화된 컴퓨팅 환경에서도 각종 디지털 자산에 안전하게 접근할 수 있도록 하는 기술

● (국내) **디지털 신분증, 암호화폐 등 최근 관심을 받거나 시장이 활발**한 분야 외에 미래의 새로운 디지털 서비스 환경을 대비한 보안 연구는 미흡한 수준

- **(분산 디지털 신원관리) DID(분산신원증명) 핵심기술 확보** 및 관련 보안 기술에 대한 연구가 ETRI 등 연구소와 산업체 중심으로 활발히 진행 중

※ 행안부의 모바일 운전 면허증 발급 등 국내 디지털 신분증 관련 서비스의 확산으로 기술 수요 증가 예상

- **(메타버스 보안)** 메타버스 산업 성장에 대한 기대감과 함께 **메타버스로 인한 부작용(프라이버시 침해, 디지털 성범죄 등) 우려**는 높으나 관련 연구 활동은 초기 단계

- **(탈중앙화 가상경제 보안)** 펜타시큐리티, 드림시큐리티 등 국내 주요 보안기업은 **암호화폐 보호를 위한 전자지갑 개발에 집중**, 탈중앙화 거래에 대한 보안기술 연구는 초기 수준

※ 스마트계약(smart contract) 보안 등 탈중앙화 거래의 요소 기술에 대한 연구는 R&D 진행 중이나 NFT(대체불가능토큰), DeFi(탈중앙화금융) 등 새로운 거래 형태의 보안 기술연구는 미흡

- **(비대면 보안) 비대면 인증, 화상회의 보안 등 관련 연구가 연구소·기업을 통해 진행**되었으나, 제로트러스트, 사이버보안 메시 등 기업 전반의 보안을 다루는 연구는 미비

※ 키오스크에서의 무자각 비대면 인증 기술, 화상회의 참석자 신원확인 및 회의자료 보호 기술 등이 연구소와 기업을 통해 연구됨

마. 사이버 범죄 대응

- (국외) 사이버 공간에서의 범죄 대응을 위한 다중 소스 증거 분석과 **범죄자 및 근원지 추적을 통한 공격 억제력 대응 기술 개발 추진**
  - **(스마트기기 디지털 포렌식)** IoT 디바이스 및 클라우드 데이터 수집을 통한 사용자 행위 중심의 다중 소스 증거수집 및 분석 기술 연구 중

    ※ 미국의 경우 웨어러블 디바이스(스마트워치)의 센서 데이터와 스마트기기(스마트폰) 데이터의 다중 소스 분석을 통해 범죄분석에 활용
  - **(다크웹 사이버범죄 근원지 추적)** 미국과 유럽에서는 다크웹 상의 범죄정보 유통 서버 취약점 등을 활용한 미공개 정보를 수집하여 은닉 서버 및 범죄자 추적과 검거에 나서고 있음

    ※ 미국 FBI는 Operation Tornado에서 NIT(Network Investigation Technique) 프로그램을 활용하여 특정 컴퓨터에 접근하는데 성공하였으며, 유럽 Europol은 다크웹 전담팀을 2018년도에 설립하고, "360도 전략"을 수립하여 다크웹 단속을 강화하고 있음
  - **(랜섬웨어 공격 근원지 추적 및 피해복구)** 가상자산 추적을 통한 랜섬웨어 해킹그룹 추적과 피해복구를 위해 백업 및 복구 속도, 그리고 백업 데이터의 안전성 보장 측면의 성능향상을 위한 기술개발 진행

    ※ 미국 FBI는 2021년 다크사이드 해킹그룹 공격으로 콜로니얼 파이프라인을 마비시킨 대형 랜섬웨어 사건과 관련해 해당 기업이 지불한 비용 중 일부인 약 230만불 상당의 비용을 환수한 바 있음

- (국내) 사이버 범죄에 대해 정보수집·공격 탐지·피해복구 등 탐지중심 기술개발로 **사이버 범죄 대응 및 추적 기술은 미흡한 수준**
  - **(스마트기기 디지털 포렌식)** 삭제파일 복구 및 암호화 해제 기법을 활용한 데이터 중심의 디바이스 증거 수집 및 분석 기술 연구 중

    ※ 스마트기기의 증거 수집을 위해 외부 인터페이스를 통한 논리적 추출 방식과 삭제파일 복구 등을 위해 플래쉬 메모리의 물리적 추출 기술을 주로 활용하며, 표준화된 분석 기술은 존재하지 않음
  - **(다크웹 사이버 범죄 근원지 추적)** 다크웹 상의 사이버 범죄 정보 연관성 분석, 프로파일링 및 암호화폐 주소추적 등의 방식을 활용한 근원지 추적 기술 개발이 시도되고 있으나, 수집 가능한 데이터의 한계가 존재함

    ※ 기업의 정보 유출 여부 및 공격 징후 파악을 위한 Threat Intelligence 분야와 OSINT 분야에 집중되어 있어, 범죄 수사를 위한 도구 개발이 시급한 상황임
  - **(랜섬웨어 공격 근원지 추적 및 피해복구)** 데이터 금고 구축을 통해 데이터 백업 및 복구 기술 개발이 추진 중이나, 랜섬웨어에 특화된 범죄 근원지 추적 기술 개발이 요구됨

    ※ 데이터금고: 중소기업의 데이터 이중화 지원을 위해 클라우드 또는 하드웨어 기반의 백업 지원

바. 융합 산업 보안

- (국외) 산업 및 국방 등의 **전 분야에서 IT와 OT의 융합보안기술과 표준화 활성화**
  - **(국방 통신 및 무기체계 보안)** 미국을 중심으로 국방 기술 선도국에서는 사이버 공격에 대응하기 위한 무인이동체 보안요구사항 및 관리규정 등을 제도화 하고 있음
  - **(해양·선박 IT+OT 융합보안)** 최근 IT와 OT 결합 대규모 자율시스템 보안에 대한 관심이 증가하고, 선진국 주도로 선박운항 타겟으로 한 사이버공격 피해와 대규모 영향을 고려한 사이버 보안 요건을 포함하는 국제 IMO 규제화 진행 중

    ※ 국제해사기구(IMO)는 선주 협회와 실질적인 규제화와 미국 USCG 또한 보안관리 심사를 통해 규제화를 진행 중이며, EU연합과 유럽국가 주도로 MUNIN, AUTOSHIP 등의 프로젝트를 통해 사이버보안 기술개발 추진 중
  - **(저궤도 위성 보안)** 영국 Surrey 대학교는 '19년부터 미국의 사이버보안 컨설팅 그룹 NCC와 인공위성 보안센터를 만들어 인공위성의 사이버 위협 분석 및 대응 연구를 추진

    ※ 민간기업 OneWeb, SpaceX, Telesat, Amazon 등 주도로 저궤도 위성을 활용한 글로벌 인터넷망 구축 사업이 활발히 진행되고 있음

    ※ 저궤도 위성통신에서의 보안 위협 유형을 살펴보면 DoS/DDoS, Hijacking, Malware, 하드웨어 백도어, OS취약점 등 기존 인터넷 기반의 통신/서비스/장치에서 발생할 수 있는 위협이 그대로 존재함

- (국내) **IT와 OT의 융합보안에 대해 민간분야 중심에서 국방으로 확대**되는 추세
  - **(국방 통신 및 무기체계 보안)** 육군 예하 드론봇전투단을 창설('18.9)하는 등 무인 전투체계 연구개발에 집중하고 있어, 무인이동체를 군에서 안전하게 활용할 수 있는 보안기술 개발 요구
  - **(해양·선박 IT+OT 융합보안)** 스마트선박에 보안기술을 접목하려는 수준으로써 장기적으로 활용되어야 하는 자율운항 등 선박 특성을 고려한 사이버 위협에 대응되는 보안 수준과는 격차가 존재
  - **(저궤도 위성 보안)** 「제2차 위성정보 활용 종합계획」의 세부추진과제 이행을 위한 '위성정보 활용 시행계획'을 매년 수립하고, '21년도 약 3,200억원 정부투자를 계획하고 있지만, 단기적으로 저궤도 위성통신 보안에 대한 연구개발이 필요

    ※ 저궤도(LEO, Low Earth Orbit) 위성통신: 고도 160~2,000Km 상공을 이동하는 위성을 통해 전세계 어디서나 이동통신을 이용할 수 있는 시스템. 저궤도 위성통신 시스템은 위성간 공중 세그먼트, 위성과 게이트웨이 간 지상 세그먼트, 사용자 세그먼트 등으로 구분됨

사. 물리환경 안전·보안

- (국외) 영상보안플랫폼의 개방화, CCTV 엣지지능의 고도화를 통해 SOC 등 사회 기반 시설과 미션-크리티컬 산업에서 영상보안의 핵심역할이 부각되고 있음

※ 온-디바이스 AI가 미래 유망 기술 트렌드로 부각되고 있음(MIT Technology Review, '22)

- **(고성능 On-CCTV 지능)** Bosch, AXIS, Panasonic 등 글로벌 CCTV 업체들은 고지능·고성능을 탑재한 엣지 AI CCTV 제품 출시 및 시장 경쟁 심화

※ 단순 객체탐지 수준을 벗어나 얼굴/차량 인식, 휴먼/차량 속성인식, Business Intelligence 등 제공

- **(개방형 영상보안플랫폼)** Bosch 등을 중심으로 기존 임베디드 리눅스 기반 폐쇄적 CCTV 환경에서 안드로이드 기반 개방형 CCTV 플랫폼으로 전환 중

※ 개방형 CCTV 플랫폼을 통해 CCTV 제조사 협조 없이도 누구나 원하는 솔루션을 개발, 탑재, 운영 가능

※ OSSA(Open Security & Safety Alliance) : Bosch, 한화테크윈, Siemens, Hisilicon 등 글로벌 CCTV 업체를 중심으로 안드로이드 CCTV 사실표준 제정 완료 및 시제품 출시('19~)

※ Azena(www.azena.com) 사이트는 CCTV용 AI 앱을 공유, 판매, 시험할 수 있는 앱-스토어 운영

- **(영상시스템 보호 확대)** 대부분 CCTV 제품에 SSL/TLS 통신채널 보호 기능이 기본 탑재되어 있으며, 일부 제품은 프라이버시 보호, 인증, 무결성, 접근 제어 기능 지원

※ AXIS는 ARTPEC-8(CCTV 전용 SoC)을 통해 Signed firmware, Secure Boot, 암호화 키 및 인증서의 안전한 저장을 위한 Edge Vault, 디바이스 인증을 위한 AXIS Device ID, 영상 무결성 보장을 위한 Signed Video 등의 기능을 제공

● (국내) 아직 서버 기반 지능형 CCTV 솔루션이 대부분이며 자율 대응·보호를 보장하는 CCTV 온-디바이스 지능은 글로벌 수준에 비해 기술 경쟁력이 낮음

- **(단순수준 On-CCTV 지능)** 영세한 국내 CCTV 제조사의 낮은 AI 기술력으로 CCTV IQ가 낮으며, 연구기관에서 개발한 경량 AI CCTV 기술을 탑재하기도 어려움

※ 국내 CCTV 제조사의 개발환경 공개·공유 없이는 고지능 솔루션 탑재, 시험, 운영이 불가능하며, 이러한 이유로 CCTV 자체 지능이 단순 탐지 수준을 벗어나지 못하고 있는 실정임

- **(개방형 영상보안플랫폼)** 한화테크윈은 Bosch, Milestone, Pelco, VIVOTEK 등과 같이 OSSA 단체를 설립하여 표준을 주도하고 있으며, 현재 시제품 제작 완료

※ 한화테크윈의 안드로이드 CCTV에 다양한 영상AI 기능을 탑재, 시험을 계획하고 있음

- **(네트워크 보안솔루션에 의존)** 원영상 복원가능한 프라이버시 마스킹/복원 기술, 실시간 경량 암·복호 기술을 개발하였으나 아직 방화벽 등 외부 보안시스템에 의존

※ 가정집, 어린이집, 수술실 등 프라이버시 민감형 서비스에서의 보안 대책이 시급하며, CCTV 디바이스 자체의 보안은 SSL/TLS 등 단순 통신채널보호 기능만 탑재되어 있으며, 이마저도 전용망에 대한 과신뢰, 영상 품질저하 우려로 사용하지 않는 경우가 대부분임

3 사이버보안 기술의 진화 방향

가. 데이터 활용 보안

- 데이터의 생산 주체인 개인의 권리를 최대한 보장하면서 자유로운 데이터 활용이 가능한 **개인데이터 신뢰·유통 기술 개발의 확산, 양자 컴퓨팅 대응 기술 개발 지속** 전망
  - **(개인 프라이버시 강화 기술)** 데이터 경제 시대 도래에 따라 개인 프라이버시 강화를 위해 민감정보 비식별화 중심 기술에서 **프라이버시 강화 컴퓨팅 기술**로 발전

    ※ (EU)GDPR, (미)CCPA, (중)개인정보보호법, (한국)데이터 3법 개정 등 개인 프라이버시 강화
  - **(양자 컴퓨팅 대응 기술)** 양자컴퓨터, AI 등 새로운 공격 기법 등장에 대응하기 위한 **암호체계 안전성 검증 및 신규 암호체계 설계 기술 연구**가 지속 될 것으로 예상

    ※ 미국 NIST는 PQC 표준 최종 3라운드 진행, '24년 최종 선정 예정
  - **(데이터 신뢰·유통 기술)** 데이터 활용 전주기에서 **데이터 생산자인 개인의 권리 보장 중심의 데이터 활용 환경 구축을 통해 데이터 산업 전반**에 활용될 것으로 전망

    ※ 동형암호 실용화를 통해 개인의 민감 데이터에 대해 데이터 활용 전주기에 걸쳐 암호화 상태를 유지하면서 활용성 제공 및 활용 목적에 특화된 고속 암호데이터 활용 기술 설계 진행

    ※ 개인의 데이터에 대한 권리 보장을 위해, 특정 기업 및 기관에 의존하지 않는 분산 환경 중심의 데이터 유통·활용 환경 구축을 통한 개인 중심의 데이터 활용 전망

나. 차세대 네트워크 보안

- 차세대 네트워크 보안에 성능향상을 위해 일부 활용되어 오던 **인공지능 기술이 보다 폭넓게 적용**될 것으로 전망
  - **(5G/5G+ 융합서비스 보안위협 대응 기술)** 초연결·가상화·분산구조의 확대에 따라 인공지능 기반의 실시간 보안위협 탐지·대응이 본격화될 전망
  - **(사설 5G/특화망 네트워크 보안 기술)** 사설 5G 구축 유형 및 서비스(공공, 국방, 제조, 물류 등)별로 특화된 맞춤형 네트워크 보안 기술로 발전
  - **(6G 네트워크 보안 내재화 기술)** 6G망/서비스 보안 위협에 따른 대응을 자율화/자동화하기 위하여 6G 네트워크 환경에서 **AI 기반 보안 분석 기능의 내재화 기술**로 발전

    ※ AI 학습엔진(ML/DL, 분산/연합학습) 플랫폼을 코어 네트워크 내부에 배치, 기기 근처 엣지에서 AI 기능 제공하는 AI 네트워크 기술 및 표준기술(NWDAF)에 대한 연구가 진행 중임

- **(인공지능 기반 지능형 보안관제 기술)** 인공지능을 활용하여 대규모의 지능적인 해킹 공격에 자동적으로 탐지/대응하기 위한 통합정보보안 시스템 기술로 발전

※ Paloalto Networks 보안 오케스트레이션, 자동화, 대응 플랫폼으로 기존 플랫폼에 위협 인텔리전스 관리 기능을 긴밀히 통합한 코어텍스 XSOAR 를 출시

- **(인공지능 기반 사이버 공격 시뮬레이션 기술)** 사이버 공격 뿐만 아니라 방어 기술에도 인공지능을 활용한 시뮬레이션 기술로 발전

다. 시스템 · 디바이스 보안

● 대량의 이기종 디바이스 간의 협업을 통한 **능동적인 보안위협 대응기술**로 진화가 예상되며, **HW 기반 공급망 보안 기술이 강조**될 것임

- **(AI기반 악성코드 분석 기술)** 악성코드를 이용한 사이버공격이 지능화됨에 따라 기존 상용백신 솔루션의 한계점을 해결하기 위한 **클라우드 기반 다중 AI 백신 기술**로 발전 전망

※ 기존의 패턴 기반 백신 엔진에서 탐지하지 못하던 수많은 변종/신종 악성코드를 AI 기술을 활용하여 분석 및 탐지하고, 단일 백신의 의존성을 해결하기 위한 연구가 진행 중임

- **(지능형 IoT 디바이스 보안 기술)** IoT 디바이스 보안위협에 노출되는 대상을 인지하고 빠른 확산을 막기 위한 클러스터링, 그룹핑, 세그먼트 기반 보안 통제 기술로 발전

※ 보안위협에 대한 시각화와 보안위협 인지 기술에 AI를 적용하는 기술로부터 더욱 고도화하여 보안위협 확산 정도를 예측하는 기술로 발전될 것으로 예상함

- **(HW/SW 공급망 보안)** PCB 레벨의 공급망 위협 분석 기술에서 **IC칩 레벨의 내부 데이터 및 코드의 안전성 검증** 기술로 발전

※ 장비 운용을 위한 펌웨어/암호키 등의 주요 정보들이 SoC(System-on-Chip) 내부에 저장되고 있어, 공급망 과정에서 장비에 대한 의도적 보안 취약점 삽입 여부를 검증하기 위해서는 SoC칩 내부 데이터의 획득 및 분석 기술이 요구됨

라. 신 디지털 플랫폼 보안

● 모든 경제활동이 현실에서 가상세계까지 확대되는 메타버스 환경에서 사용자의 디지털 자산 및 프라이버시 보호를 위한 **새로운 패러다임의 보안 신기술 등장** 전망

※ 신 디지털 플랫폼은 이용기기(PC/스마트폰 → XR/IoT), 데이터 소유주체 (기업 → 개인), 통제방식 (중앙집중형 → 분산화)의 변화를 고려한 보안 신기술 요구

- **(분산 디지털 신원관리) 데이터주권 및 디지털 지갑의 보안 기능(분실 대비 백업·**

복구, 인증 및 개인키 보호 등)을 강화하기 위한 연구가 활발히 진행될 것으로 예상

※ 사용자 직접 통제에 의해 관리되는 디지털 신분증, 암호화폐, 디지털 자산 등의 확산은 사용자 관리 부담 및 정보 유출로 인한 금융피해 등을 초래할 수 있어 이에 대한 대응책 필요

- **(메타버스 보안) 메타버스 '빅브라더' 우려에 대응**하기 위한 프라이버시 보호 기술과 **아바타·디지털자산에 대한 인증** 기술, **신종 디지털 범죄 대응** 기술 등이 등장할 전망

※ 메타버스 디바이스로 센싱된 이용자 신체·행동·주변 정보, 메타버스 상에서의 구매·방문자·위치 등 행위정보는 기존 서비스에서 다루지 못한 규모와 종류의 개인정보로 구성되어 있어 프라이버시 보호 대책 마련 없이는 메타버스 서비스 확산의 허들로 작용

※ 메타버스 상에서 이루어지는 신규 사이버 범죄(아동성범죄, 피싱, 신원(아바타) 사칭 등)를 사생활침해 없이 모니터링 하고 탐지할 수 있는 기술 등이 필요

- **(탈중앙화 가상경제 보안)** 가상경제에서 거래의 신뢰성을 제공하기 위해 **가상경제 부정거래(사기, 자금세탁 등) 방지** 기술, 디지털 저작권 보호 기술 등 연구 추진 전망

※ 중앙 감시·보호 기관의 역할이 제한적인 가상경제에서 부정거래 방지를 위해 정상 이용자 피해 없이 자금세탁 등의 불법 이용자에 대한 탈중앙화 거래 추적 기술, 개인간 거래 신뢰성 보장 기술 등 필요

- **(비대면 보안)** 제로트러스트 보안, 비대면 클라우드 서비스 보안, 무인화 보안 및 비접촉 인증 등 기술의 지속적인 **고도화 및 실서비스 적용** 전망

※ 비대면 서비스의 일상화로 공격 대상·접점 증가, 무인화 등 서비스 환경변화에 대한 대응 기술 필요

마. 사이버 범죄 대응

● 사이버 안전망에 대한 요구가 증대되면서 범죄 억제력 강화를 위한 **범죄자 추적 및 사이버 복원력 기술이 확대**될 전망

- **(스마트기기 디지털 포렌식)** 디바이스 중심에서 웨어러블 디바이스를 포함하는 IoT 디바이스 및 클라우드 데이터의 표준화된 다중 소스 연계 증거 수집 및 분석 기술로 확대

※ 웨어러블 디바이스 및 스마트 홈 IoT의 확대에 따라 다중 소스 연계 증거 수집 및 분석 기술의 필요성은 확대될 것으로 예측됨

- **(다크웹 사이버 범죄 근원지 추적)** 다크웹 상의 범죄정보 유통 은닉서비스 서버 근원지 추적과 불법 이용자를 추적하는 다크웹 근원지 분석 및 추적 기술 개발의 추진 예상됨

※ 범죄자 추적을 위한 주요 정보는 단순 크롤링을 통해 획득하기 매우 어렵기 때문에, 이러한 한계를

극복하여 추가 정보를 수집하고 이를 기반으로 근원지 추적이 가능한 실질적 수사도구가 필요함

- **(랜섬웨어 공격 근원지 추적 및 공격 피해복구)** 랜섬웨어 서비스 제공 해킹 조직의 프로파일링을 통해 발견된 랜섬웨어의 근원지를 추적하는 기술로 진화 예상

※ 랜섬웨어 코드, 공격기법, 서버IP, 이메일 주소 등의 공격 정보를 분석하고 DB화함으로써 동작 특징을 분석하고 이를 바탕으로 탐지 및 차단 등 신속한 대응이 가능한 관련 기술개발이 필요함

바. 융합 산업 보안

- SoC **디지털 가속화**에 따른 주요 기반시설 및 국방 분야에 적용 가능한 IT와 OT 융합보안의 활성화 전망

- **(국방 통신 및 무기체계 보안)** 미래戰 양상과 미래 전장환경 변화에 따라 인공지능 기반 무인전투체계 구축은 전 세계적인 추세로써, 안정적이고 신뢰할 수 있는 운영을 위해 강력한 보안기술이 필수적으로 선결되어야 함

- **(해양·선박 IT+OT 융합보안)** 선박은 IT와 OT의 결합 네트워크로 구성돼 사이버 침해 대응뿐만 아니라 다양한 센서·통신 시스템의 데이터 보호와 안전성, 취약점 분석 등 장기적 관점에서 다양한 보안기술의 융합 예상

※ 스마트선박 자체의 선박 시스템은 AIS 등 기본 식별자와 위치정보가 그대로 공개되는 구조이며, 이러한 수집정보와 센서정보에 기반하여 자율운항 형태로 진화되므로 다양한 공격에 매우 취약한 구조로서 온보드시스템 및 연결된 전용채널에 대한 보안성과 안전성을 높일 필요가 있음

- **(저궤도 위성 보안)** 국내외 우주산업 활성화에 따른 저궤도 위성 통신·서비스 증대로 저궤도 위성 사이버위협에 대한 보안 대책이 가시화될 것으로 예상

※ 저궤도 위성 보안 관련 주요 핵심기술: 저궤도 위성시스템 인프라 보안위협 분석 기술, 위성간 공간 세그먼트 상의 암호통신 보호 기술, 위성통신 게이트웨이 및 네트워크관리센터(NMC) 상의 네크워크 보안 기술, 위성통신 및 서비스 단말 상의 인증 및 프라이버시 보호 기술 등

사. 물리환경 안전·보안

- HW와 SW가 상호 종속되지 않는 안드로이드 기반 CCTV 플랫폼 활성화에 따라 **초지능을 보유한 CCTV 디바이스 확대** 전망

- **(개방형 영상보안 생태계)** 자유로운 SW 앱 개발, CCTV 탑재 및 연동 시험을 통해서 고성능 AI CCTV 기술이 현장 적용될 수 있는 **개방형 영상보안 생태계 조성** 전망

※ 폐쇄형 CCTV의 단순 전처리 수준을 탈피해서 선도기술이 CCTV에 탑재될 수 있는 토대 마련

- **(자율보호가 내재화된 초신뢰 영상보안플랫폼)** 프라이버시/미션-크리티컬 영상보안

시스템이 자율적인 보안위협 방어 능력을 보유한 **On-CCTV 보안지능 강화** 전망

※ 백도어, 해킹 등 다양한 보안위협을 스스로 감지, 방어, 대응 등 자율방어 기능이 내재화된 CCTV 제품/체계, 영상 유출에 강인한 영상 전주기 보호, 다중 영상보안시스템간 자율 증명·협업 등

※ 국내외 CCTV, DVR 등 11,700여대의 장비가 'Mozi봇넷' 감염('22), 월패드 해킹('21) 등 심각한 프라이버시 침해 범죄 증가는 물론 CCTV가 활용되는 다양한 융합산업에 치명적 피해 발생 우려

- **(On-CCTV 자율·초지능 확대)** 고성능 HW 기반 CCTV가 스스로 다양한 안전위협을 감지, 예측, 협업, 공동대응하는 **On-CCTV 자율 초지능 제품/솔루션 확대** 전망

※ 특정(지정된) 위험 이벤트 감지가 아닌 전반적인 발생 상황을 묘사함으로써 범용 AI CCTV로 발전

- **(중대 사회안전재난 대응 강화)** 중대재해처벌법 시행('22.01)으로 산업현장에서 각종 안전사고, 재난·재해 대응을 위한 AI CCTV의 역할 중요성 강화

※ 미국 등 선진국의 경우 EHS(Environment, Health & Safety) 관리플랫폼 고도화, AIoT 기반 안전관리 플랫폼 구축으로 산업현장 재난사고 발생 억제 및 조기 대응으로 피해를 최소화

※ 기존 사회안전(범죄, 사고 등) 중심에서 붕괴·폭발, 화재(산불, 방화 등), 침수, 해양오염 등 산업적·자연적 재난·재해 대응으로 확대되고 이에 대한 관리 주체의 책임소재 강화 추세

- **(전국 CCTV IQ 통합관리플랫폼)** 전국(Nation-wide) 영상보안시스템의 지능을 지속적으로 최적화 유지·관리할 수 있는 **중앙집중형 영상보안 AI 통합관리 체계**로 발전

※ 탈중앙 신뢰 연합학습, 보안 리소스 공유/분배/관제 등을 통한 SOC, 주요안전시설, 산업현장의 CCTV IQ의 지속적 최적화 등 국가 주요 시설안전지능의 통합관리 필요(AIMS)

※ 각 AI CCTV 운영 시스템에서 급속히 발전하는 다양한 AI 기술을 개별적으로 최적화하는 것은 매우 어려워, 각 도메인별 통합관리 필요(예: 국방 과학화경계감시를 위한 CCTV AI 통합관리플랫폼)

IV 사이버보안 시장 및 산업 동향

1 글로벌 사이버보안 시장 전망

- 사이버보안은 1장의 〈그림 1-1〉과 같이 정보보호와 동일한 개념으로 여겨지고 있으며, 따라서, 본 보고서에서는 사이버보안과 정보보호 시장을 포괄하여 소개

- 해외 주요 시장조사 전문기관들에서는 글로벌 사이버보안 시장 규모가 증가할 것으로 예측(〈표 4-1〉)

  - 2020년대에 연평균 최소 9.5%에서 최대 14.5%까지 성장할 것으로 전망

표 4-1 글로벌 사이버보안 시장 전망

시장조사기관	전망
Mordor Intelligence (2021)	2021년 글로벌 사이버보안 시장은 약 1,329억 달러이며, 2022년부터 2027년까지 연평균 14.5% 성장할 것으로 전망
Grand View Research (2021)	2020년 글로벌 사이버보안 시장은 약 1,674억 달러이며, 2021년부터 2028년까지 연평균 10.9% 성장할 것으로 전망
Allied Market Research (2022)	2020년 글로벌 사이버보안 시장은 약 1,973억 달러이며, 2021년부터 2030년까지 연평균 9.5% 성장하여 4,786억 달러에 이를 것으로 전망
MarketsandMarkets (2021)	2021년 글로벌 사이버보안 시장은 약 2,179억 달러이며, 2021년부터 2026년까지 연평균 9.7% 성장하여 3,454억 달러에 이를 것으로 전망
Fortune Business Insights (2021)	2021년 글로벌 사이버보안 시장은 약 1,397억 달러이며, 2022년 1,558억 달러 2029년 3,763억 달러 연평균 13.4%
Research and Markets (2022)	2020년 글로벌 사이버보안 시장은 1,562억 달러이며, 2021년부터 2026년까지 연평균 14.5% 성장하여 3,522억 달러에 이를 것으로 전망

※ 출처: 각 기관 자료, 저자 재정리

- 정보통신기획평가원의 "ICT R&D 기술로드맵 2025"에서는 차세대보안* 세계 시장이 2018년부터 2026년까지 연평균 15.3% 성장하여 5,839억 달러에 이를 것으로 전망

  * 4차 산업혁명 시대 진입과 전산업의 초연결화·디지털화·지능화로 인해 야기되는 고도의 사이버 위협과 같은 부작용을 해소하여 실생활에서 국민 안전과 자산을 보호하는 신규기술을 포함

  - 세계 시장 규모는 2018년 2,508억 달러이며, 정보보안 분야의 시장 비중이 약 60.9%로 가장 높고 물리보안이 33.5%, 융합보안이 5.6%으로 나타남

  - 융합보안 시장의 경우 비중은 가장 작으나 CAGR 28.5%의 높은 성장률을 보이며 급격히 성장할 것으로 전망

표 4-2 차세대보안 분야 중분류별 시장전망 (단위: 백만달러, 십억 원, %)

구분		2018	2019	2020	2021	2022	2023	2024	2025	2026	CAGR
정보보안	세계	152,656	168,227	185,386	204,295	225,134	248,097	273,403	301,290	332,022	10.20%
	국내	3,083	3,278	3,815	4,442	5,170	6,019	7,007	8,156	9,495	16.41%
물리보안	세계	84,150	90,293	96,884	103,957	111,546	119,689	128,426	137,801	147,860	7.30%
	국내	7,035	7,280	7,833	8,428	9,069	9,758	10,499	11,297	12,156	7.60%
융합보안	세계	14,004	17,995	23,123	29,713	38,181	49,063	63,046	81,014	104,103	28.50%
	국내	700	900	1,156	1,486	1,909	2,453	3,152	4,051	5,205	28.50%
전체(합계)	**세계**	**250,810**	**276,514**	**305,393**	**337,966**	**374,861**	**416,849**	**464,875**	**520,105**	**583,986**	**15.33%**
	국내	**10,818**	**11,457**	**12,804**	**14,355**	**16,148**	**18,230**	**20,658**	**23,504**	**26,856**	**17.50%**

※ 출처: 정보통신기획평가원(2020), ICT R&D 기술로드맵 2025

- 디지털 전환의 가속화 및 사이버 공격 방식의 정교화 등으로 인해 사이버보안에 대한 수요가 급격히 증가
  - 코로나19로 인해 재택근무가 늘어나고 디지털 전환이 가속화되면서 다양한 사이버 위협이 증가
  - 스마트 기기 사용자 수의 급격한 증가, 기업들의 클라우드 컴퓨팅 채택 증가, IoT 와 같은 다양한 디지털 기술의 산업 적용 등으로 인해 보안 솔루션에 대한 수요가 늘어남
- 공공 및 민간 부문에서 보안 솔루션에 대한 수요가 급격히 증가하면서, 벤처캐피털의 투자가 사이버보안 회사로 유입되고 있음
  - 2021년 6월 기준 사이버보안 관련 스타트업이 전세계적으로 99억 달러를 투자받았으며, 이는 2020년 투자금 총액의 96%에 달함[13)]

- 디지털 전환, 코로나19 등의 환경변화로 인해 사이버 위협이 증가하면서 글로벌 사이버보안 시장은 지속적으로 성장할 전망
- 글로벌 사이버보안 시장에서 정보보안 분야가 가장 비중이 높으며, 융합보안 분야는 현재는 비중이 낮으나 향후 급격히 성장할 것으로 예측됨
- 벤처캐피털의 사이버보안 관련 스타트업에 대한 투자가 전세계적으로 급격히 증가

13) Pitchbook(2021.06.17.), Cybersecurity startups near record funding as hacks take spotlight

2 주요국 사이버보안 시장 및 산업 동향

가. 미국

- 미국의 사이버보안 산업은 전세계를 주도하고 있으며, 사이버보안 환경도 매우 우수
  - 미국의 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)는 2020년 기준 100으로 전세계 1위를 기록[14)]
  - 미국에서 사이버보안 산업은 국가 기간산업으로서 강조되고 있으며, 미국 연방정부 및 국방부에서는 사이버보안 관련 투자를 지속적으로 늘리고 있음

표 4-3 2020년 글로벌 사이버보안 지수(GCI) 순위[15)]

순위	국가명	지수	순위	국가명	지수
1	미국	100	19	벨기에	96.25
2	영국	99.54	20	이탈리아	96.13
2	사우디아라비아	99.54	21	오만	96.04
3	에스토니아	99.48	22	핀란드	95.78
4	한국	98.52	23	이집트	95.48
4	싱가포르	98.52	24	인도네시아	94.88
4	스페인	98.52	25	베트남	94.59
5	러시아 연방	98.06	26	스웨덴	94.55
5	아랍에미리트	98.06	27	카타르	94.5
5	말레이시아	98.06	28	그리스	93.98
6	리투아니아	97.93	29	오스트리아	93.89
7	일본	97.82	30	폴란드	93.86
8	캐나다	97.67	31	카자흐스탄	93.15
9	프랑스	97.6	32	덴마크	92.6
10	인도	97.5	33	중국	92.53
11	터키	97.49	33	크로아티아	92.53
12	호주	97.47	34	슬로바키아	92.36
13	룩셈부르크	97.41	35	헝가리	91.28
13	독일	97.41	36	이스라엘	90.93
14	포르투갈	97.32	37	탄자니아	90.58
15	라트비아	97.28	38	북마케도니아	89.92
16	네덜란드	97.05	39	세르비아	89.8
17	노르웨이	96.89	40	아제르바이잔	89.31
17	모리셔스	96.89	41	키프로스	88.82
18	브라질	96.6	42	스위스	86.97

※ 출처: ITU(2022), Global Cybersecurity Index 2020

14) ITU(2022), Global Cybersecurity Index 2020
15) GCI는 국가 정보보안과 관련한 입법, 기술조치, 전략 및 제도, 훈련 및 R&D, 국제협력 등 5개 분야를 평가하여 산정

- 미국의 사이버보안 시장 규모는 2021년 기준 약 541억 달러 규모이며, 글로벌 사이버 보안 시장 대비 비중은 40.9%로 가장 높음[16)17)]
  - 2022년부터 연평균 7.4%로 성장하여 2026년에는 약 781억 달러 규모에 이를 전망
- 미국의 사이버보안 산업은 시장 규모, 인프라 개발, 혁신, R&D 활동 등 전반적인 면에서 전세계에서 가장 앞서 있음
  - 대다수 산업이 지능형 지속 위협(Advanced Persistent Threat, APT) 대응 및 계정 및 액세스 관리(Identity and Access Management, IAM) 활동에 대한 가시성을 확보하기 위해 고급 보안 솔루션을 채택
  - 때문에 사이버 보안 솔루션을 개발하는 기업들에게 많은 기회가 주어지고 있으며, 시장경쟁력을 확보하기 위해 기업들의 연구개발 노력도 활발
  - 핵심 과학기술이 집약되어 있는 국가인 만큼 사이버 위협의 가능성이 높고, 코로나19로 인해 디지털 전환이 촉진되면서 사이버보안 솔루션에 대한 수요 증가
- 미국의 사이버보안 시장은 특정 기업이 경쟁적 우위를 가지지 않는 경쟁적인 시장 구도를 보임
  - NortonLifeLock[18)], Cisco Systems, Palo Alto Networks, Fortinet, McAfee, Rapid7, Imperva 등 다양한 기업들이 치열하게 경쟁 중
  - 최근 사이버보안 관련 스타트업들이 급부상하고 있으며, 대표적인 스타트업으로는 Beyond Identity, Confluera, Netskope, Exabeam, Lacework, Rubrik 등이 있음

나. 중국

- 중국의 글로벌 사이보보안 순위는 미국, 영국, 독일, 일본, 한국 등 글로벌 주요국에 비해 다소 낮은 편[19)]
  - 중국의 2020년 글로벌 사이버보안 지수(GCI)는 92.53으로 세계 33위(〈표 4-3〉)
  - 영국 국제전략문제연구소(IISS)에서는 중국의 사이버보안 역량이 미국에 비해 10년가량 뒤처져 있다고 분석하였으며, 이는 중국의 인터넷 감시·검열 시스템인 “만리방화벽

16) 한국인터넷진흥원(2022), 2021 글로벌 정보보호 산업시장 동향조사
17) 세계 시장 규모는 약 1,321억 달러
18) Symantic Corporation이 2019년 11월 사명 변경
19) ITU에서는 GCI 상위 50위권에 속한 국가를 “사이버보안을 위해 매우 노력하는 국가”로 분류

(防火长城)"[20] 때문인 것으로 추정됨('21.6)

- 중국의 사이버보안 시장은 2021년 기준 약 99억 달러 규모로, 전년 대비 19.1% 증가하였으며, 글로벌 사이버보안 시장의 7.5%를 차지하고 있음[21]
  - 2022년부터 연평균 19.7%로 성장하여 2026년에는 약 242억 달러 규모에 이를 전망
  - 미국에 비해 글로벌 사이버보안 시장 대비 비중은 낮은 편이나, 시장 성장세가 높음
- 5G 상용화, 디지털 산업 육성 및 높은 인터넷 사용자 규모 등을 기반으로 하여 사이버보안 시장은 지속적으로 성장할 것으로 전망됨
  - 중국 정부는 5G를 상용화하고('20), 빅데이터, IoT, AI, 클라우드 등을 디지털 기술 관련 산업을 중점 산업으로 육성하고 있기 때문에, 향후에도 사이버보안 솔루션에 대한 수요가 지속적으로 증가할 것으로 예측됨
- 중국 사이버보안 시장의 주요 사업자로는 NSFocus(綠盟科技), Venutech(启明星辰), Westone(衛士通), Tianrongxin(天融信), Sangfor Technoloogies, Anity Labs, DBAPP Security Ltd.(安恒信息) 등이 있음

다. 영국

- 영국의 2020년 글로벌 사이버보안 지수(GCI)는 99.54로, 1위 미국에 이어 전세계 2위를 기록(<표 4-3>)
  - 2018년에는 GCI 1위를 차지하는 등 우수한 사이버보안 환경을 지속적으로 유지
  - 국가적으로 정보보호정책을 강화하면서 보안 관련 기기·솔루션·소프트웨어 등에 대한 수요가 지속적으로 증가할 것으로 예측됨
- 영국의 사이버보안 시장은 2021년 기준 약 86억 달러로, 글로벌 사이버보안 시장의 6.5%를 차지함[22]
  - 2022년부터 연평균 9.3%로 성장하여 2026년에는 약 135억 달러 규모에 이를 전망
- 자국 내 사이버보안 산업도 높은 수준이나, 수요의 대부분을 수입에 의존하고 있어 기업 간 경쟁이 치열

20) 중국이 사회안정을 이유로 자국 내 인터넷을 규제하기 위해 강제하는 법적 조치와 기술의 결합을 의미. 선별된 외국 웹사이트로의 접근 차단 및 국경을 넘는 인터넷 트래픽 속도를 낮춤
21) 한국인터넷진흥원(2022), 2021 글로벌 정보보호 산업시장 동향조사
22) 한국인터넷진흥원(2022), 2021 글로벌 정보보호 산업시장 동향조사

- 특히, 정보보안 분야의 경우, 다국적 사이버보안 컨설팅사, 전문 ICT 사업자, 다국적 HW/SW 벤더, VAR(Value Added Reseller) 등이 단독 또는 컨소시엄 형태로 입찰에 참여하면서 치열한 경쟁 구도 형성

- 영국 사이버보안 시장의 주요 사업자로는 Sophos, Intercede, Sentry Bay, Exclusive Networks 등이 있음
  - 영국의 사이버보안 스타트업들 역시 두각을 나타내고 있으며, 대표적인 스타트업으로는 Darktrace, CybSafe, Callsign 등이 있음

라. 일본

- 일본의 2020년 글로벌 사이버보안 지수(GCI)는 97.82로, 전 세계 7위를 기록하였으며, 미국(1위), 영국(2위), 한국(4위) 등의 주요국보다는 낮은 편(〈표 4-3〉)

- 일본의 사이버보안 시장은 2021년 기준 약 71억 달러로, 글로벌 사이버보안 시장의 5.4%를 차지[23)]
  - 2022년부터 연평균 8.1%로 성장하여 2026년 105억 달러에 이를 전망

- 코로나19로 인한 디지털 전환 확대 및 사이버 위협의 증가 등으로 인해 사이버보안 솔루션에 대한 필요성이 증가하였으나, 아직까지 사이버보안 관련 의식은 저조한 수준
  - IDC Japan의 조사에 따르면 2021년 1월 기준 일본 기업 833개 기업 중 60%가 정보보안 투자 예산이 별도로 존재하지 않는다고 응답

- 일본 사이버보안 시장의 주요 사업자로는 Trend Micro, Fujitsu, Hitachi, Vinx 등이 있음

마. 한국

- 한국의 2020년 글로벌 사이버보안 지수(GCI)는 98.52로, 전 세계 4위를 기록하였으며, 타 주요국에 비해 우수한 사이버보안 환경을 보유(〈표 4-3〉)

- 한국의 사이버보안 시장은 2018년 약 10.8조 원에서 연평균 17.5% 성장하여 2026년에는 약 26.8조 원 규모로 증가할 전망(〈표 4-2〉)[24)]

23) 한국인터넷진흥원(2022), 2021 글로벌 정보보호 산업시장 동향조사

- 2018년 기준으로 글로벌 사이버보안 시장의 경우, 정보보안 시장의 비중이 가장 큰 반면, 한국 시장은 물리보안 시장의 비중이 65%로 가장 높게 나타남

  ※ 정보보안 28.5%, 물리보안 65.0%, 융합보안 6.5%

- 융합보안 분야는 6.5%로 매우 비중이 낮으나, 2026년까지 연평균 28.5%로 급격히 성장할 전망

● 한국의 정보보호 산업은 꾸준히 성장하고 있으나, 기반 기술이 부족하여 응용제품 개발 위주의 전문 중소기업 중심으로 발전

- 2020년 기준 국내 정보보호 기업 수는 정보보안 531개, 물리보안 752개로 총 1,283개이며, 2017년 총 897개(정보보안 332개, 물리보안 565개)에 비해 1.43배 증가[25)]

- 자본금 100억 이상의 업체가 3.4%(44개), 50억 미만의 업체가 93.2%(1,196개)로 중소 및 벤처기업이 대부분을 차지함

● 한국 사이버보안 시장의 대표적인 기업들로는 안랩, 오픈베이스, 윈스, 이글루시큐리티, 한국정보인증, 이니텍, 이스트소프트, 드림시큐리티 등이 있음

- 안랩의 경우 2020년 1,726억 원의 매출을 올리며, 보안 분야 20개 상장기업[26)] 중 가장 높은 매출을 기록

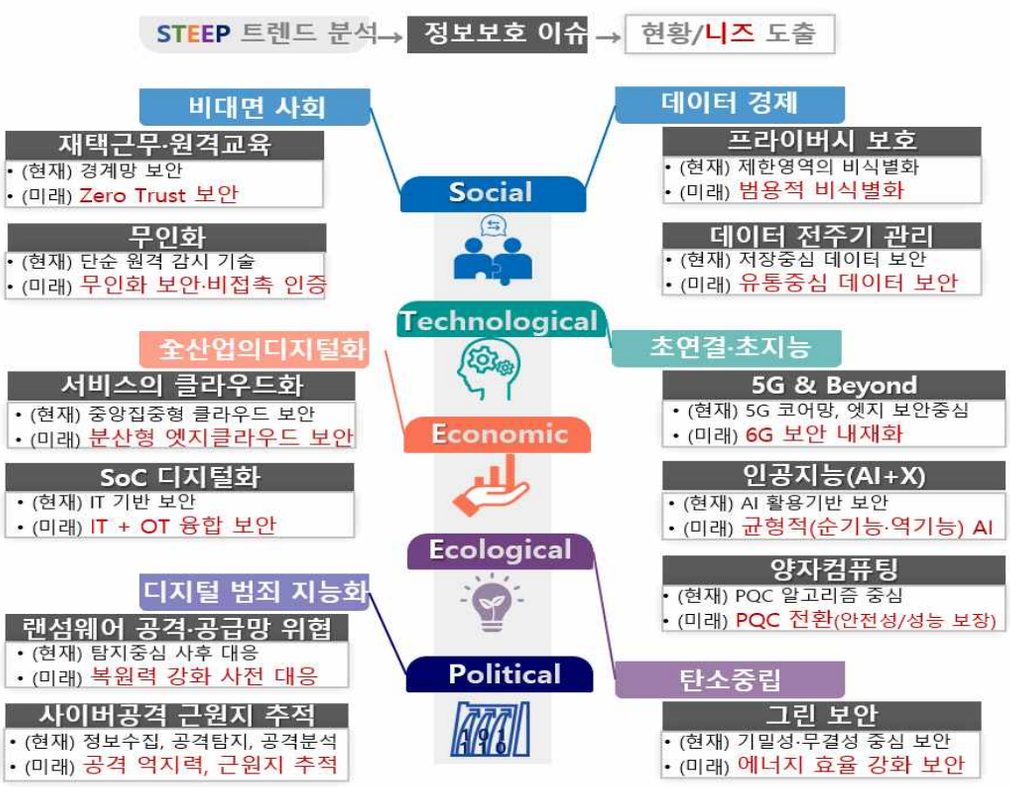
- 글로벌 사이버보안 시장은 미국이 주도하고 있으며, 미국은 시장 규모, 인프라 개발, 혁신, R&D 활동 등 전반적인 면에서 전세계에서 가장 앞서 있음
- 중국은 GDP 규모에 비해 글로벌 사이버보안 시장에서의 비중이 낮은 편이나, 향후 급격히 성장할 것으로 예상됨
- 영국은 사이버보안 산업의 수준이 비교적 높으며, 기업 간 경쟁이 치열한 양상을 보임
- 일본의 경우, 디지털전환으로 인해 사이버보안에 대한 필요성이 증가하고 있으나, 아직까지 사이버 보안 관련 의식이 저조
- 한국은 기반 기술의 부족으로 응용제품 개발 위주의 중소 및 벤처기업 중심으로 발전

24) 정보통신기획평가원(2020), ICT R&D 기술로드맵 2025
25) 한국정보보호산업협회(2021), 2020 정보보호산업 실태조사
26) 드림시큐리티, 라온시큐어, 시큐브, 안랩, SGA솔루션즈, 오픈베이스, 윈스, 이글루시큐리티, 이니텍, 이스트소프트, 지니언스, 지란지교시큐리티, 케이사인, 코닉글로리, 파수, 파이오링크, 한국전자인증, 한국정보인증, 마이더스AI, 한컴위드

V 사이버보안 분야 R&D 이슈

- 사이버보안 분야와 관련한 거시환경 변화를 분석하기 위해 STEEP 분석 프레임을 활용하여 주요 이슈를 도출
  - STEEP 분석은 미래예측 전문가인 Jerome C, Glenndl 고안한 거시환경 분석 프레임으로 Social(사회), Technical(기술), Economic(경제), Ecological(환경), Political(정책)의 5가지 분야에 대한 종합적 분석을 수행하는 기법
  - STEEP은 현재의 잠재적인 문제점, 기회, 신규 시장, 신제품 및 신서비스 출시, 미래전략 기획 등에 광범위하게 활용되는 기법
  - ETRI 정보보호연구본부(2022)에서 수행한 사이버보안 분야 STEEP 분석을 통해 5개 분야별 거시환경 변화와 이에 따른 사이버보안 분야의 이슈를 정리한 결과는 다음의 〈그림 5-1〉과 같음

그림 5-1 사이버보안 분야 STEEP 분석 결과



※ 출처: ETRI 정보보호연구본부(2022), 거시환경 분석으로 본 Cyber Security R&D 2022, 원내 세미나 발표자료.

- (Social) '비대면 사회'의 확산으로 인해 재택근무 및 원격교육이 보편화되고, 각종 사회시스템이 무인화되는 트렌드가 더욱 강해질 전망이며, '데이터 경제' 시대의 도래로 개인 프라이버시 보호 문제가 부각되고, 데이터 전주기 관리에 대한 요구가 강화될 전망
  - 비대면 사회의 확산은 'Zero Trust 보안' 이슈 및 '무인화 보안과 비접촉 인증' 관련 기술에 대한 수요를 자극할 것으로 예상됨

    ※ Zero Trust(영신뢰) 보안 : '아무것도 신뢰하지 않는다'를 전제로 한 사이버 보안 모델로, 내부에 접속한 사용자에 대해서도 무조건적으로 신뢰하지 않고 검증하는 것을 기본으로 하는 개념. '제로 트러스트'는 전체 시스템에서 안전한 영역이나 사용자는 전무하다는 것을 기본 전제로 한 뒤, 내부자 여부와 상관 없이 인증절차와 신원확인 등을 철저하게 검증하고 접속 권한 부여 뒤에도 그 접근 범위를 최소화함
  - 데이터 경제 시대의 도래로 제한영역의 비식별화를 넘어 '범용적 비식별화' 기술에 대한 요구가 자극될 것이며, 현재의 저장 중심 데이터 보안 보다는 '유통 중심의 데이터 보안'이 보편화 될 것으로 예상됨

- (Technological) 제4차 산업혁명의 가속화로 '초연결', '초지능', '초실감' 기술의 진화가 빨라지고, 이를 기반으로 새로운 '디지털 플랫폼'들이 보편화되며, '양자 컴퓨팅' 시대의 도래가 가시화될 전망
  - 5G 코어망 및 엣지 보안 중심의 초연결 분야 사이버보안 이슈가 6G의 상용화(2018년 이후) '6G 보안 내재화' 중심으로 변화할 전망
  - 인공지능의 보편화로 'AI+X' 현상이 가속화되면서 '균형적 AI' 활용을 위한 보안 이슈가 더욱 강하게 대두할 것으로 예상됨
  - 메타버스 환경의 보편화로 새로운 디지털 플랫폼들이 증가함에 따라 이용기기가 PC 및 스마트폰에서 XR 기기 중심으로 변화하고, 데이터의 소유 주체가 기업 중심에서 개인 중심으로 이동하며, 통제방식이 중앙집중형에서 분산화로 변화함에 따라 '디지털 신분증' 등 '분산형 인증'과 '데이터 주권' 이슈가 부각할 전망
  - 양자컴퓨팅 시대의 도래를 예고하는 연구결과들*이 속속 발표되면서 기존 '공개키 암호체계(RSA, ECC)의 붕괴'가 예상되는 만큼, 'PQC Engineering' 및 'PQC 전환 기술' 등 양자컴퓨팅 고도화보다 앞선 초신뢰 암호기술 확보에 대한 필요성 증대

    * 구글은 '19년에 53큐빗 시커모어 '양자 우월성' 결과를 발표했고, IBM은 '23년에 1000+ 큐빗의 양자컴퓨터 개발 로드맵을 발표할 예정

    ※ PQC(Post-Quantum Cryptography; 포스트 양자암호) : 양자컴퓨터를 이용한 해킹으로부터 안전한 비대칭 키 암호 알고리즘

- (Economic) 디지털 전환 현상의 보편화로 '전산업의 디지털화'가 촉진되고, 디지털 기술 기반의 '데이터 경제 시스템'이 확산될 전망
  - 도로·철도 등 교통기간망과 전기·통신 및 상하수도와 같은 산업 제어시스템 분야에서의 사이버 위협이 본격화될 전망
  - 과거 100여 년이 사회간접자본(SOC)을 구축하는 시대였다면, 향후 100여 년은 SOC를 안전하고 효율적으로 관리하는 시대가 될 가능성이 농후하며, 디지털 기술을 기반으로 한 SOC 관리가 보편화되는 추세
  - 이러한 'SOC 디지털화' 현상은 현재의 IT 기반 SOC 보안을 'IT와 OT(Operation Technology)의 융합보안' 형태로 변화시킬 것으로 예상됨
  - 전산업의 디지털화가 촉진되는 과정에서 IoT 기기들이 대량으로 도입될 것은 분명하기 때문에 개별기기 인증 및 보안보다는 'Massive IoT 기기 검증' 방식의 사이버 보안 기술에 대한 필요성이 증대할 것으로 전망됨
  - 데이터 경제 시대의 본격화는 앞서 서술한 Social 분야에서의 전망과 마찬가지로, '유통 중심의 데이터 보안' 및 '개인 프라이버시 강화' 기술에 대한 필요성을 증대시키고 있음

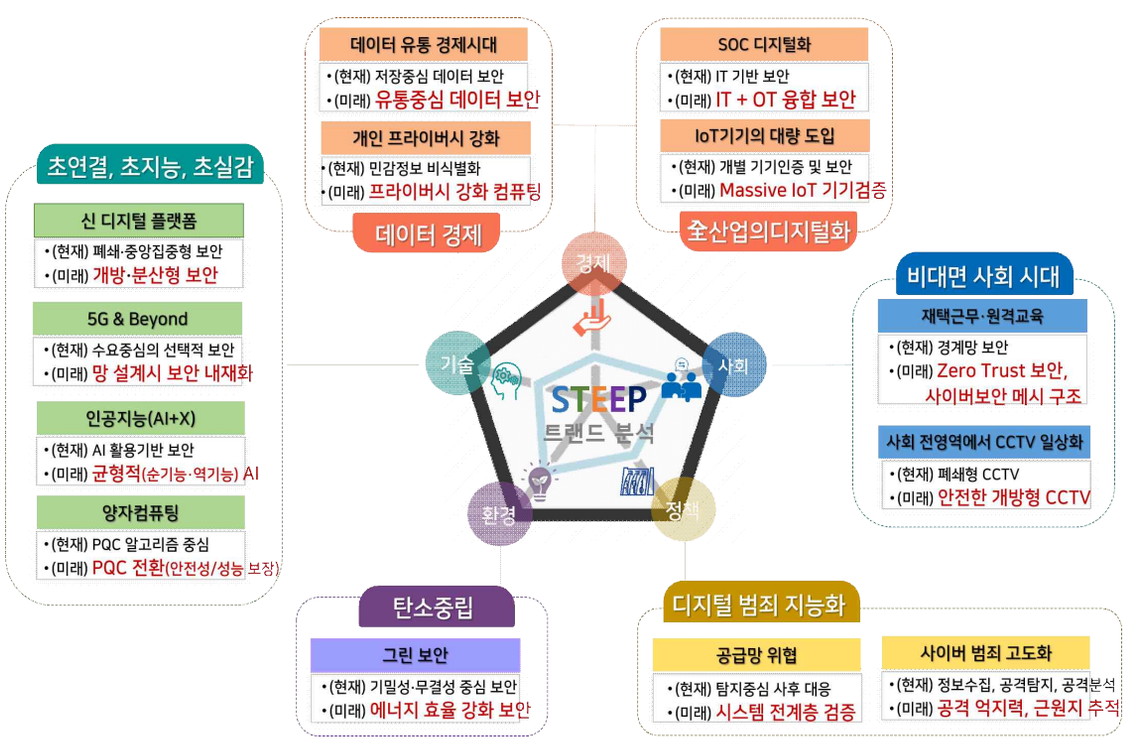
- (Ecological) 전지구적 문제로 부각 중인 지구 온난화 및 환경 오염 문제들로 인해 '탄소중립' 이슈가 국가적으로 중대한 정책 이슈화되었으며, 이로 인해 '에너지 효율 컴퓨팅 환경'에 대한 요구도 증대
  - AI 중심의 디지털 전환이 가속화되면서 글로벌 데이터센터에서 사용하는 전력량이 200TWh 수준으로 급증했는데, 이는 전세계 전략 사용량의 1%에 해당하는 규모
  - 이러한 전략 사용량 급증 문제에 대처하기 위해 구글, IBM 등은 AI 프로세서에 에너지 효율성을 제고하기 위한 '근사 컴퓨팅' 기술을 적용하기 시작

    ※ 근사 컴퓨팅(Approximate Computing) : 일반적으로 컴퓨터는 항상 100%의 정확성을 갖는 연산과 정보처리를 해야 한다고 생각하지만, 영상 처리, 머신러닝, 웹 검색 등 다양한 컴퓨팅 분야에서는 정확도의 손실이 일부 있더라도 원하는 결과를 얻을 수 있는 확률이 높음. 따라서 '근사값'을 기반으로 컴퓨팅을 수행할 경우 에너지 소모를 절감할 수 있다는 개념
  - 근사 컴퓨팅 등 에너지 효율 시스템에서의 관련 보안 기술을 선점할 필요성이 높아지고 있으며, 향후 급증하는 디지털 전환 관련 전력량 문제에 대비하기 위한 '그린 보안 생태계' 구축 이슈가 대두

- (Political) '국가 공급망 위협' 우려가 심화되고, '사이버 범죄'가 고도화되면서 사이버 보안 문제는 이미 국가·기업의 생존과 관련된 정책적 이슈로 자리매김
  - 국가가 지원하는 해킹그룹에 의한 공급망 공격 빈도가 증가하고, SW 및 HW 공급망을 통한 랜섬웨어 확산 문제가 심각해지며, 라이브러리 취약점 문제로 공급망 보안위협이 증대되는 상황
  - 해외에서 수입하는 장비에 대한 국가 차원의 보안성 평가 기술 확보가 필요하며, 기밀이 요구되는 국가 정부기관의 장비에 대한 안정성 검증을 위한 기술도 필요
  - 최근 사이버범죄 자금흐름에 대한 추적방지를 위해 다크웹 및 암호화폐 사용이 증가하는 추세이고, 랜섬웨어 제작/공급/수익배분이 고도로 분업화되고 조직화된 형태로 발생 중
  - 따라서 '시스템 전계층에 대한 보안 검증' 기술 확보 및 '사이버범죄 억제력 강화와 범죄 근원지 추적' 기술이 요구되는 상황

- 이상 STEEP 프레임을 통해 분석한 사이버보안 분야의 거시환경 변화상을 기반으로 관련 R&D 이슈를 도출한 결과는 다음의 〈그림 5-2〉와 같이 정리 가능

그림 5-2 거시환경 변화 분석에 기반한 사이버보안 분야 R&D 이슈



※ 출처: ETRI 정보보호연구본부(2022), 거시환경 분석으로 본 Cyber Security R&D 2022, 원내 세미나 발표자료.

참고문헌

◆ 국내자료

과학기술정보통신부(2018), 4차 산업혁명 대응 사이버 보안 핵심기술개발사업(안).

과학기술정보통신부 (2020), 디지털경제의 튼튼한 '방역체계' 구축한다.

관계부처합동(2018), '데이터 산업 활성화 전략'.

관계부처합동(2019), 국가 사이버안보 기본계획.

관계부처합동(2020), 제2차 정보산업진흥계획 : 디지털 경제 전환을 정보보호산업 성장의 기회로(2021~2025).

관계부처합동(2021), 글로벌 기술패권 경쟁에 대응한 국가필수전략기술 선정 및 육성·보호 전략.

관계부처합동(2022), 디지털 대전환 시대 정보보산업의 전략적 육성 방안.

국가사이버안전관리규정 제2조의 3.

국가안보실(2019), 국가사이버안보전략.

김상배(2017), 국가 사이버 안보 전략의 국제비교:한반도 주변4국과 유럽 주요 3국의 사례.

김상배(2019), 사이버 안보의 국가전략 2.0... 사이버 안보와 미중 기술패권 경쟁.

김정곤,나승권,장종문,이성화(2015), EU 디지털 단일시장 전략의 주요 내용과 시사점. 대외정책연구원.

박민숙(2020), 중국의 사이버보안 정책 연구.

박민숙·이효진(2020), 중국의 사이버보안 정책 연구, 연구자료 20-03, 대외경제정책연구원.

박상돈 외(2017), 사이버안보 법제도의 의의에 대한 새로운 이해.

박상돈, 김규동, 김소정 '사이버안보 법제도의 의의에 대한 새로운 이해', 보안공학연구논문지, Vol.14. No.2 (2017).

박성림(2019), 국가 주도형 사이버보안 거버넌스의 확산: 중국 및 동남아 국가 사례를 중심으로.

심진보·유영상, 정보보안 및 보호 : 사이버 보안을 중심으로, 핵심가치 분석서 20219-09, 한국전자통신연구원.

이원상(2020), 주요 국가들의 사이버보안법 동향이 주는 시사점 고찰.

정보통신기획평가원(2020), ICT R&D 기술로드맵.

정성영(2022), 일본의 ICT R&D 포트폴리오.

한국군사문제연구원(2021), 2022년도 일본의 '주요 방위력 개선' 내용.

한국법령정보원(2018), 사이버안보법제 고찰.

한국인터넷진흥원(2018), 해외 주요기반보호 등 사이버보안법제 비교법 연구.

한국인터넷진흥원(2022), 2021 글로벌 정보보호 산업시장 동향조사.

한국정보보호산업협회(2021), 2020 정보보호산업 실태조사.

ETRI(2022), 거시환경 분석으로 본 Cyber Security R&D 2022, 원내 세미나 발표자료.

IITP(2020), ICT R&D 기술로드맵 2025.

KOTRA(2019), 2019 미국 사이버보안시장 동향과 시사점.

IITP(2021), 최근 중국의 사이버보안 정책 동향: 입법 규제를 중심으로, 과학기술&ICT 정책·기술동향, No. 199.

KOTRA(2020), 2021년 美 대통령 예산안 개요 및 시사점.

IITP(2019) 미국·일본의 사이버보안 예산 및 정책분석.

KOTRA(2018), 트럼프 정부의 국가 사이버보안 전략 및 시사점.

KOTRA(2020), EU 디지털전략 정책안 발표, 디지털시대 EU의 전략은?.

KOTRA(2022), 2021년 미국 사이버 보안 산업.

◆ 국외자료

Allied Market Research(2022), Global Cyber Security Market – Opportunities and Forecast, 2021-2030

Department of energy(2021), Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats, APRIL 20, 2021

Fortune Business Insight(2021), Cyber Security Market Forecast, 2022-2029

Gartner(2021), Gartner's Top Strategic Technology Trends for 2022

Gartner(2021), Predicts 2022 : Cyber-Physical Systems Security — Critical Infrastructure in Focus (https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/)

Grand View Research(2021), Cyber Security Market Size, Share & Trends Analysis Report By Component, By Security Type, By Solution, By Services, By Deployment, By Organization, By Application, By Region, And Segment Forecasts, 2021 – 2028

IISS(2021), Cyber Capabilities and National Power: A Net Assessment.

ITU(2022), Global Cybersecurity Index 2020.

MarketsandMarkets(2021), Cybersecurity Market – Global Forecast to 2026

Mordor Intelligence(2021), Global Cybersecurity Market – Growth, Trends, Covid-19 Impact, And Forecasts (2022 – 2027)

OMB, Analytical Perspectives-Budget of the U.S. Government(Fiscal Year 2020),2019.2

Peter Gwynne(2020), Bipartisan bill aims to revamp National Science Foundation

Research and Markets(2022), Cybersecurity Market – Growth, Trends, COVID-19 Impact, and Forecasts (2022 – 2027)

◆ 웹사이트

NTIS 국가과학기술지식정보서비스, https://www.ntis.go.kr/

◆ 신문기사

KOTRA 해외시장뉴스(2021.12.29.), “2021 일본의 정보 보안 산업”, https://dream.kotra.or.kr/kotranews/cms/news/actionKotraBoardDetail.do?pageNo=19&pagePerCnt=10&SITE_NO=3&MENU_ID=200&CONTENTS_NO=1&bbsGbn=403&bbsSn=403&pNttSn=192618&pStartDt=&pEndDt=&sSearchVal=&pRegnCd=&pNatCd=&pKbcCd=&pIndustCd=&sSearchVal=

KOTRA 해외시장뉴스(2022.01.04.), “2021년 미국 사이버 보안 산업”, https://dream.kotra.or.kr/kotranews/cms/news/actionKotraBoardDetail.do?SITE_NO=3&MENU_ID=200&CONTENTS_NO=1&bbsSn=403&pNttSn=192645

PitchBook(2021.06.17.), “Cybersecurity startups near record funding as hacks take spotlight”, https://pitchbook.com/news/articles/cybersecurity-startups-near-record-funding-as-hacks-take-spotlight

보안뉴스 (2021.03.23.), “주요 보안분야 20개 상장사 2020년 성적표 공개... 2/3가 매출 올랐다”, https://www.boannews.com/media/view.asp?idx=95820

조선일보(2022.01.11.), “경제분야 극단 美中, 사이버 보안 영역으로 전쟁 확대”, http://it.chosun.com/site/data/html_dir/2022/01/10/2022011001702.html

저자소개

심진보 ETRI 지능화융합연구소 기술정책연구본부 기술전략연구센터장 책임연구원
e-mail: jbsim@etri.re.kr Tel. 042-860-6213
원용숙 ETRI 지능화융합연구소 기술정책연구본부 기술전략연구센터 책임연구원
e-mail: wys@etri.re.kr Tel. 042-860-5153
홍아름 ETRI 지능화융합연구소 기술정책연구본부 기술전략연구센터 선임연구원
e-mail: areumh@etri.re.kr Tel. 042-860-0742
홍수지 ETRI 지능화융합연구소 기술정책연구본부 기술전략연구센터 박사후연구원
e-mail: sjhong0924@etri.re.kr Tel. 042-860-3965
김익균 ETRI 지능화융합연구소 정보보호연구본부장
강유성 ETRI 지능화융합연구소 정보보호연구본부 미래암호공학연구실장
조남수 ETRI 지능화융합연구소 정보보호연구본부 미래암호공학연구실 기술총괄
김건우 ETRI 지능화융합연구소 정보보호연구본부 신인증물리보안연구실장
김수형 ETRI 지능화융합연구소 정보보호연구본부 신인증물리보안연구실 기술총괄
문대성 ETRI 지능화융합연구소 정보보호연구본부 네트워크시스템보안연구실장
김종현 ETRI 지능화융합연구소 정보보호연구본부 네트워크시스템보안연구실 기술총괄
최병철 ETRI 지능화융합연구소 정보보호연구본부 보안취약점분석연구실장
강동호 ETRI 지능화융합연구소 정보보호연구본부 보안취약점분석연구실 기술총괄

사이버보안 분야 동향 및 이슈

발행처 한국전자통신연구원 지능화융합연구소 기술정책연구본부 + 정보보호연구본부
발행일 2022년 6월 30일

www.etri.re.kr

본 저작물은 공공누리 제4유형:
출처표시+상업적이용금지+변경금지 조건에 따라 이용할 수 있습니다.

Electronics and Telecommunications Research Institute

34129 대전광역시 유성구 가정로 218
TEL.(042) 860-6114 FAX.(042) 860-6504