GISC 2024

Global ICT Standards Conference 2024

2024. 11. 4.(MON) ~6.(WED)

ELTOWER GRACE Hall 6F

(세션4) 차세대보안: 안전한 디지털 미래를 위한 표준

사이버보안 R&D 정책 및 추진방향

정현철 정보보안PM, 정보통신기획평가원

ICT Standards and Intellectual Property :
Inclusive Innovation

주최 과학기술정보통신부 특허청 주관 국립전파연구원 TTA IITP KEA kisto ETRI

DX와 사이버위협의 증대

» 공격 위협 확대

**사이버공격으로 인한 피해가 개인, 기업 → 국가로 확대,
사회 혼란, 국가간 분쟁 유발 등 국가 안보 위협**

– `24년 세계경제포럼(WEF) **'사이버안보 불안'**을 글로벌 10대 리스크 선정

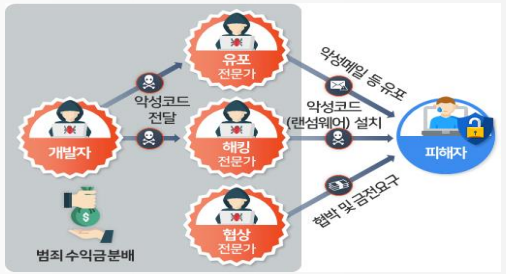
①잘못된 정보 및 허위정보, ②극심한 기상이변, ③사회적 양극화, **④사이버안보 불안**, ⑤국경간 무력 충돌, ⑥경제적 기회 부족, ⑦인플레이션, ⑧비자발적 이민, ⑨경기침체, ⑩환경오염

– 선진국 중심 **'사이버보안' 을 주요 국가안보전략 요소**로 선정

– **美**, 주변 동맹국들 간 주요 협력 분야에 **'사이버보안' 포함**

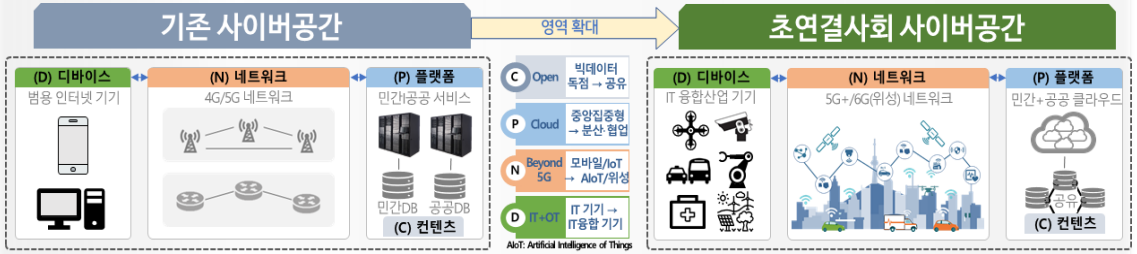
» 공격방식의 고도화 · 산업화

**(고도화) 탐지·방어가 어려운 최신 AI(ChatGPT 등)기반 공격
(산업화) 서비스형 랜섬웨어(RaaS) 등 해킹 서비스 제공**

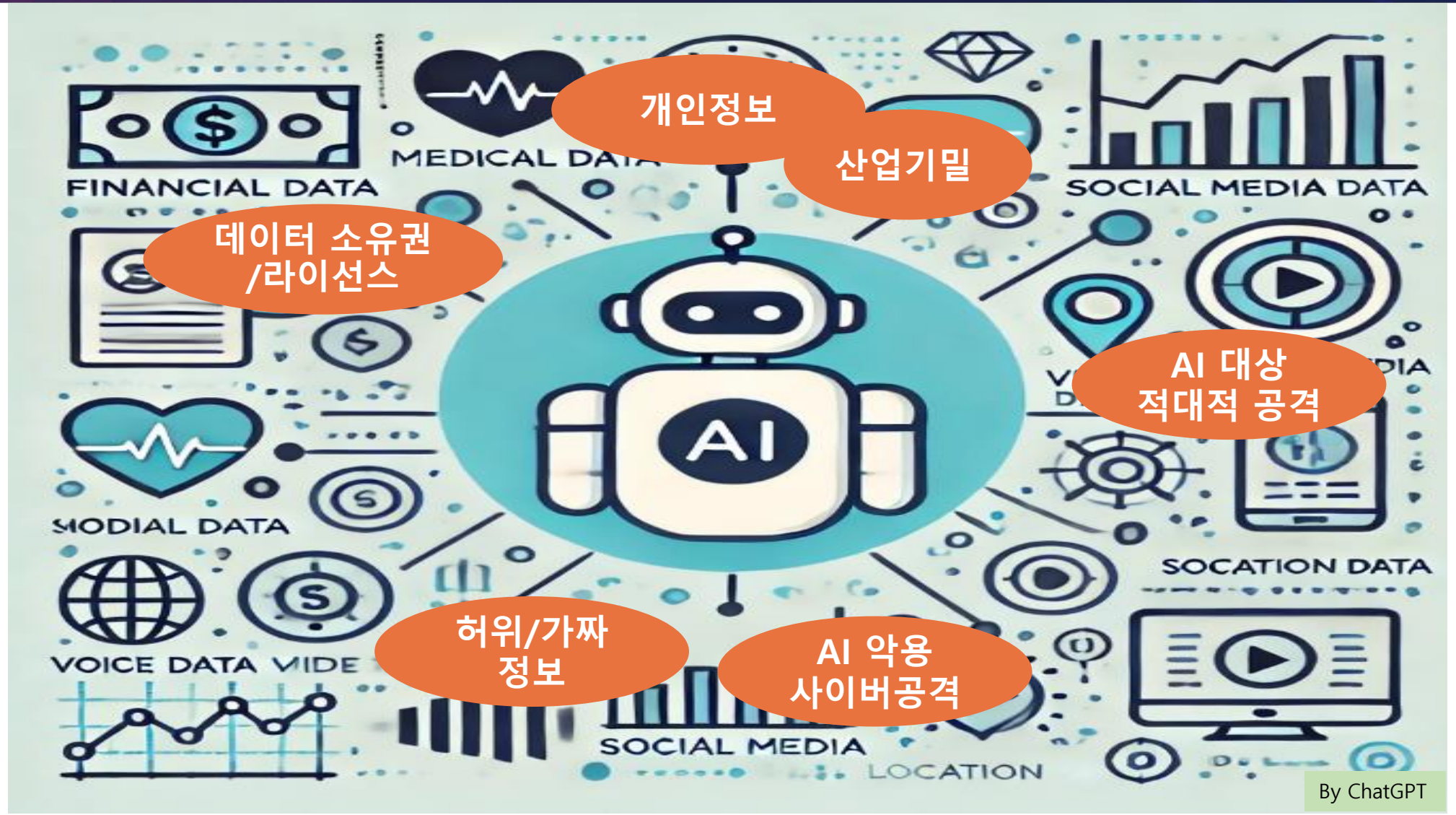


» 공격 대상 확대

**디지털 대전환, 팬데믹 상황 지속 등으로
사이버공간 확장, 확장된 공간 = 공격 대상**



사이버위협, DX시대를 넘어 AX시대로



보안, 누구의 잘못인가?


VULNERABLE SOFTWARE
VULNERABLE SOFTWARE
공격자
SW개발자
보안담당자
By ChatGPT

해외 사이버보안 정책

미국 National Cybersecurity Strategy(2023. 3.)

▌추진전략 ▐

01	02	03	04	05
주요 기반시설 방어	위협 행위자 저지 및 무력화	보안/복원력 촉진을 위한 시장의힘 형성	복원력 있는 미래에 투자	국제 파트너십 구축

미국 NCS Implementation Plan(2023. 7.)

- 국가 사이버 사고대응계획 업데이트
- Combat Ransomware
- SW bill of materials (SBOM)
- 주요 사이버보안 표준 주도
- 국제 사이버공간 및 디지털 정책 전략

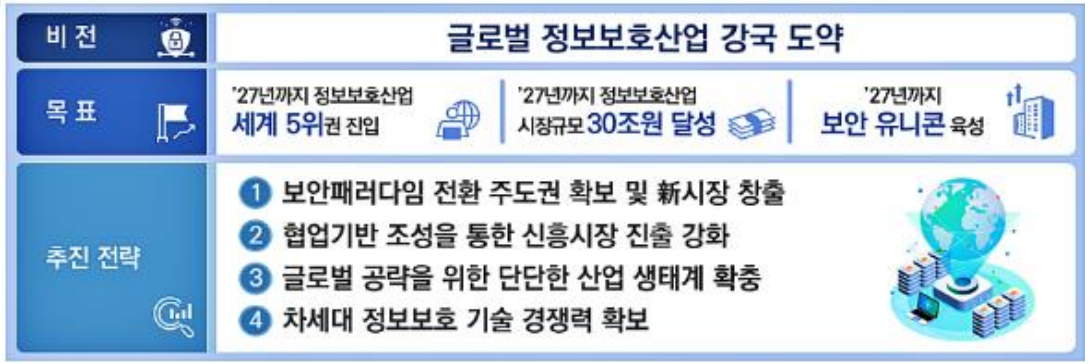
국내 사이버보안 정책

[국가 사이버안보 기본계획(2024. 9.)]

▌5대전략 ▐

01	02	03	04	05
공세적 사이버 방어활동 강화	글로벌 사이버 공조체계 구축	국가 핵심인프라 사이버 복원력 강화	신기술 경쟁우위 확보	업무 수행기반 강화

[정보보호산업의 글로벌 경쟁력 확보전략(2023. 9.)]



[대한민국 사이버안보 정책방향(2024. 9.)]

01	02
MLS 전환	AES 허용

RSA 2024로 본 사이버보안 기술/산업 동향

- 공유, 연대, 협력
- Innovation
- AI Powered Cybersecurity
- Cloud Native Security
- 통합보안, API 보안
- Zero Trust Security

사이버보안 개념 및 기술범위

정보보호 및 全 산업의 초연결화, 디지털화로 인해 야기되는 고도의 사이버위협 대응 등 실생활에서 국민의 안전과 자산을 보호하는 신기술 포함

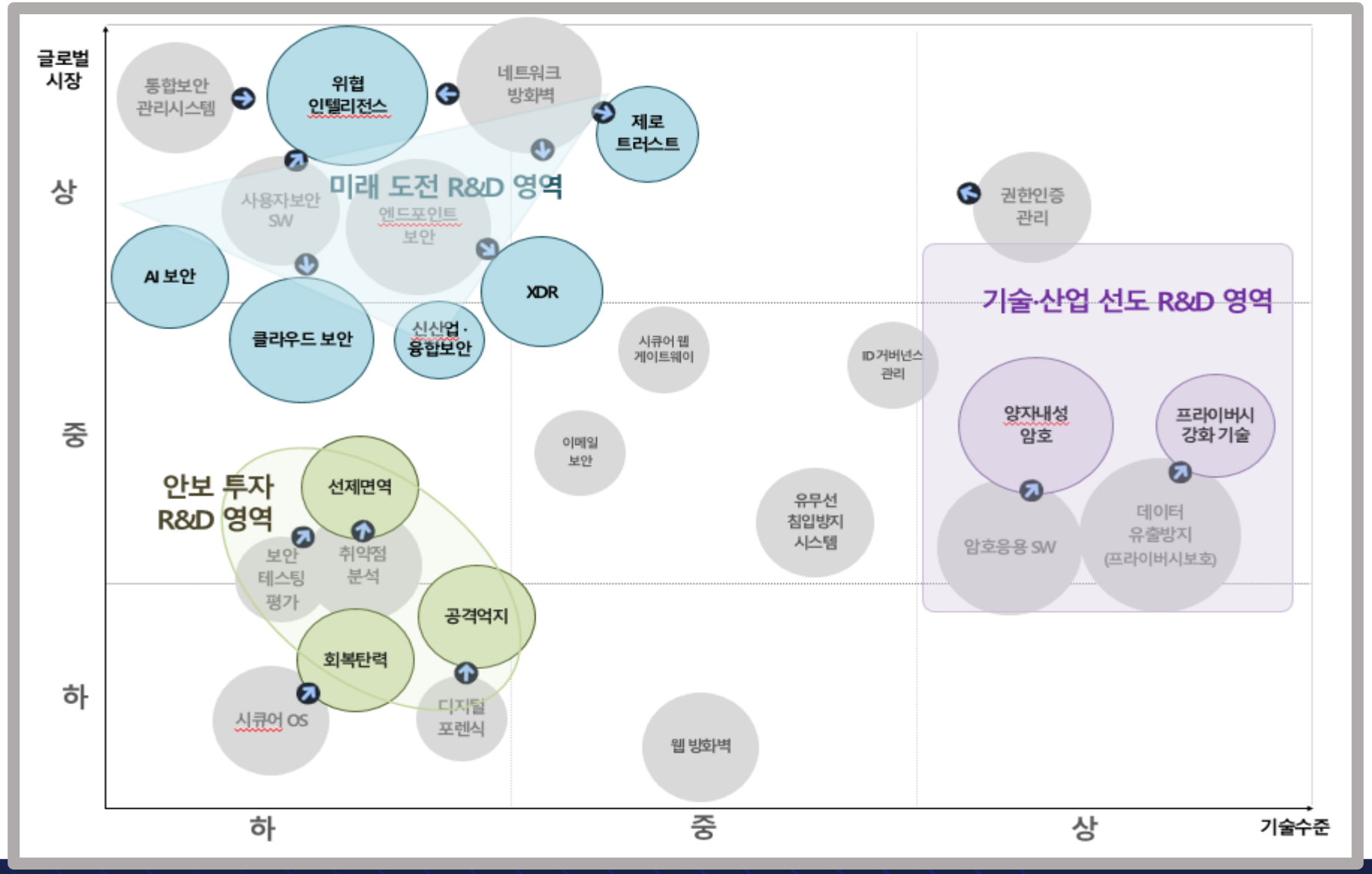
인공지능 등 기술 발전에 따라 사이버보안 영역 확장 중, 산업과 ICT융복합 가속화에 따라 사이버보안 대상도 점차 확산

12대 국가전략기술 – 사이버보안 -

중점 기술 분야

01	데이터 AI	데이터를 안전하고 신뢰성 있게 활용할 수 있도록 하며, AI 순기능 강화 및 AI 역기능 대응을 위한 융합 집힌 보안 핵심기술
02	네트워크 클라우드	초공간 · 초지능 · 초신뢰 통신 인프라의 보안 위협을 최소화, 새로운 응용 서비스의 신뢰성과 안전성을 보장하기 위한 기술
03	디지털취약점 분석 · 대응	부품, 장비 및 SW 제조 및 공급 과정 전주기 대상으로 하는 보안 위협 탐지 및 검증 등 신위협 대응을 위한 기술
04	신산업 가상융합	현실의 물리환경과 가상의 사이버환경이 일상에 공존하며, 산업분야 특성에 따라 정보보안과 물리보안을 융합하여 적용하는 기술

사이버보안 R&D 전략맵


글로벌 시장
상
중
하
통합보안 관리시스템
위협 인텔리전스
네트워크 방화벽
제로 트러스트
미래 도전 R&D 영역
사용자보안 SW
엔드포인트 보안
AI 보안
XDR
클라우드 보안
신산업·융합보안
시큐어 웹 게이트웨이
이메일 보안
안보 투자 R&D 영역
선제면역
보안 테스팅 평가
취약점 분석
공격억지
회복탄력
시큐어 OS
디지털 포렌식
웹 방화벽
유무선 침입방지 시스템
ID 거버넌스 관리
권한인증 관리
기술·산업 선도 R&D 영역
양자내성 암호
프라이버시 강화 기술
암호응용 SW
데이터 유출방지 (프라이버시보호)
하
중
상
기술수준

사이버보안 R&D 현황(2024년)

GISC 2024
Global ICT Standards Conference 2024

미래도전 R&D

541억원

- AI for Security
  Security for AI
- 클라우드 보안·XDR
- …

미래경쟁력 확보

기술산업선도 R&D

157억원

- 양자 내성 암호
- 고성능 동형 암호
- …

기술 주도·시장 확장

안보 투자 R&D

355억원

- SW 공급망 보호
- 사이버 복원력
- …

안보·안전 기반 마련

국제협력 R&D

83억원

주요 기술 선도국과의

공동 연구 + 인력 파견 + 수출 지원

글로벌 사이버 위협 공동 대응

ICT R&D 기술로드맵 2030

GISC 2024
Global ICT Standards Conference 2024

중점 기술	2025년	2027년	2030년
공통보안	AI기반 유해 콘텐츠 대응, 양자전환대응		AI 신뢰 기술, 양자환경 암호공격방어
디지털취약점 분석·시스템보안	클라우드환경 공급망, 신종범죄포렌식		하이브리드 환경 공급망, AI기반 이상행위대응
네트워크·클라우드보안	클라우드 API 보안, 제로트러스트		6G 이동통신보안, AI기반 보안관제
물리·융합보안	개방형 영상보안, 위성 취약점 탐지/대응		UAM인증 접근통제, 위성 실시간 보안탐지

공통보안

- 양자위협대응 고신뢰 암호전환
- 클라우드 네이티브 인증·인가
- 프라이버시보호 데이터활용
- AI 통제기술

- 양자저항 전자서명 인증서 설계구현
- 클라우드 네이티브(CN) IAM
- 차분 프라이버시 / 동형암호 결합 개인정보 활용
- AI 기반 유해 콘텐츠 대응
- AI 신뢰성 모니터링 / 제어
- 양자 내성암호 취약성 검증
- 지속인증을 위한 마이크로서비스
- 데이터 유출탐지 양자연산위탁
- 6G/위성통신 등 양자저항성 내재화
- CN-IAM 동적 오케스트레이션
- 연합기계학습을 위한 분산데이터 암호화
- AI 신뢰성 자율 통제 기술

디지털취약점 분석·시스템보안

- 능동형 보안위협수집·분석
- 신종범죄 대응 디지털포렌식
- 사이버범죄 인텔리전스·역추적
- 공급망 보안

- 디셉션 구축, 사이버 공격 증적 자료 확보기술
- IoC 수집, 공격시나리오, 공격 분석 / 침해공격 Attack group 및 Campaign 분석
- 단말 기기 내부데이터 접근 및 보호기법 /차세대 인프라 환경 디지털증거 수집, 분석
- 안티포렌식 자동 탐지 및 능동 대응
- 가상자산 거래 흐름 난독화 분석
- 사이버공격 전술·기법 분석, 인프라 역추적 대응
- LLM기반 이상행위 대응
- SW 공급망 전주기 보안 내재화
- 하이브리드 환경에서 SW 공급망 보안 검증 자동화, 플랫폼 펌웨어 복원력

네트워크·클라우드보안

- 차세대 이동통신 보안
- 개방형 무선네트워크 보안
- 클라우드 네이티브 보안
- Full Automation 보안관제

- 위성 공격표면분석, 취약점 탐지
- 저궤도 위성통신보안
- 초지능 6G 이동통신 보안
- 지능형 O-RAN 보안
- 개방형 프론트홀 보안
- 클라우드 API 보안 /컨테이너 플랫폼보안
- 클라우드 네이티브 애플리케이션 보호 플랫폼 (CNAPP)
- 인공지능 기반 위협탐지 / 워크플로우 기반의 자동 대응
- 위협헌팅 /인공지능 기반 분석, 보안 하이퍼오토메이션

물리·융합보안

- 고부가가치지능형CCTV
- 사용자중심 가상융합보안
- 고신뢰 모빌리티 보안
- 위성 우주 사이버전자보안

- 개방형 영상보안플랫폼 / 협업기반 통합 물리 보안모델
- 자기주권형 개인정보 디지털
- UAM 비행체 통신 채널 암호화
- 인공위성 공격표면 분석/네트워크, 펌웨어 취약점 탐지
- 보안·보호 지능 자율 탑재/적용 보안 시스템
- 가상환경에서의 프라이버시 보존 분산·개방형 데이터 유통 서비스 플랫폼
- UAM 센서 공격 탐지 및 비정상 실행 방지
- AI기반 위성-지상국간 위협 예측·탐지·대응/위성 데이터 실시간 보안 탐지

2025년 기획 방향(1)

- 미래혁신 기술 개발
  - AI·클라우드 등 신기술을 기반으로 글로벌 시장에 도전할 수 있는 미래 혁신 기술 개발
- 수요기반 기술 개발
  - CISO와 보안기업 등 수요기관(기업)이 필요로 하는 사이버보안 기술 개발에 주력
- 규제 및 패러다임 변화 대응
  - 공급망보안, AI법, 능동방어, 다층보안체계(MLS) 등 국내외 규제 및 패러다임 변화에 신속히 대응할 수 있는 기술 확보

2025년 기획방향(2)

'24년 기획 결과

● 총 53개 신규과제 기획(67,570백만원)

- **데이터·AI 보안** (8개)
  - 양자 보안, 생성형 AI 보안, 동형암호 등
- **디지털취약점 보안** (11개)
  - SW 공급망 보안, 의료기기 취약점 보안 등
- **네트워크·클라우드 보안** (12개)
  - 5G 특화망 보안, 클라우드 보안 프레임워크 개발 등
- **新산업융합 보안** (10개)
  - 영상 보안, 전기차 충전기 보안, 인공위성 보안 등
- **국방부 협력 과제** (4개)
  - 무인이동체 보안, 국방 특화 사이버보안 등
- **국제협력** (8개)
  - (미국) 국토안보부(DHS), NIST, RAND 연구소 등
  - (스위스) 취리히 공과대학교
  - (핀란드) 오울루(Oulu) 대학교

'25년 기획 방향*

● 총 9개 신규과제 기획(9,000백만원)

- **데이터·AI 보안**
  - 양자대칭암호 전환 기술, AI 생성 허위정보대응, Security for AI 기술 등
- **디지털취약점 보안**
  - 위협헌팅 디셉션 기술, SW 생태계 의존성 및 위협평가 기술 등
- **네트워크·클라우드 보안**
  - 안전한 API 연계 및 안전성 검증 기술 등
- **新산업융합 보안**
  - 고부가가치 영상보안 기술, 선박/우주 보안 등

* 기술수요를 기반으로 기술기획위원회(9월~12월)를 통해 확정예정

THANK YOU