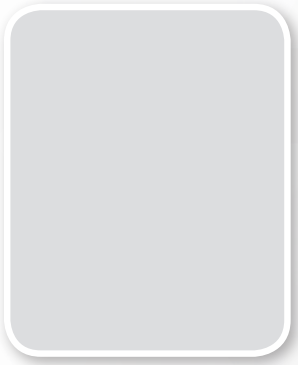


KAIST 전자학부
김광조 교수

MESIA

S

MESIA 미래전략

(안전산업 : 정보보안 분야)

세부분야

국가재난안전통신망의 장기간 보안성 보장 산업 발전 전략

1

연구 개요

■ **연구 목적**

○ 추격자전략이 필요한 분야에서 미래 新 성장 동력 창출전략

– 정보보안 영역은 미래 지속 가능한 성장을 위해 추격자(fast follower)전략을 구사해야 하는 분야로 다른 영역과 융합을 통해 발전 가능. 우선 선진국의 관련 사례를 분석하여 글로벌 트렌드를 인식한 후 최근 우리 사회에서 이슈가 되는 분야에 대해 진단이 필요. 이를 토대로 미래 30년을 예측하여 여타 기술 발전 추이에 부합하면서도 장기간 활용할 수 있는 정보보안 新 사업 성장 동력을 창출할 수 있을 것으로 판단됨

○ 보안이 바탕이 된 방재 및 안전 구현 방안 제시

– 그동안 방재 및 안전 분야는 실생활에 가장 밀접하지만 평소에는 중요성을 느끼지 못해 해외에서도 보안과 별도로 발전해 오며 효율성만 추구하는 경향이 있었음. 국내에서도 2014년 한국수력원자력 해킹 사건으로 원자력발전소 도면이 유출되어 국민적인 불안감을 초래하는 등 물리적으로 분리되어 안전하리라 믿고 있었던 원자력 발전 시설에서 보안 문제가 발생하여 크게 이슈가 됨

○ 국가재난안전통신망(이하 재난망) 구축 추진 관련 장기간 보안성을 유지하고 지속 발전 가능한 산업 분야 발굴 및 시너지 효과 극대화 도모

– 우리나라에서는 2003년 대구 지하철 화재 참사 후 재난망 구축 필요성이 제기되었으나

정상적으로 추진되지 못한 채 시간을 허비하였고, 2014년 세월호 침몰 시 단일화된 통신망 부재로 적절히 대응하지 못한 사건을 계기로 11년 만에 재난망 구축이 다시 추진되고 있음. 그런데 향후 수십 년 이상 사용할 재난통신망에 최신 보안기술이 적용되지 않으면 고유의 목적을 달성할 수 없으며, 관련된 새로운 산업 영역 개척 또한 불가함

■ **연구 필요성**

○ '안전'과 '보안'은 국민의 삶에 직접적으로 영향을 미치는 반면, 관심은 소홀

– '안전'은 세월호 사건처럼 국민의 생명과 직결되어 있고 돈으로 환산 불가한 가치를 지니지만 평소에는 느낄 수 없고, 사고가 발생했을 때만 실감할 수 있다는 특성이 있음. 단, 사고가 한 번 발생하면 대부분 대형사고로 직결되며, 복구에 천문학적 예산이 소요되는 등의 문제점을 보유하고 있음

– 정보보안 역시 국민 안전과 직결되는 경우가 상당하나 평소에는 중요성을 인식하지 못하고, 정보유출 사고 발생 시 후속조치 수준에서 답보하는 실정이며, 언론 등에서 문제를 제기하는 해당 취약점에 대해서만 땜질식 처방으로 조치하는 등 근본적인 문제점을 해결하지 못해 관련 산업 발전에도 한계가 있음

○ 안전과 보안이 융합될 경우, 새로운 성장 동력 개척 가능성 제고

– 안전 분야는 보안을 바탕으로 해야 지속 성장 가능한 영역으로 인식될 수 있으며, 장기적으로는 시스템 구축비용도 절감할 수 있음. 보안은 국민 안전 및 국가 안보와 융합될 수 있을 때 그 본연의 가치를 인정받고 시너지 효과를 발휘할 가능성이 높아짐

– 안전 산업과 보안 산업이 상생할 수 있는 영역을 찾도록 노력해야 하며, 이는 미래 우리나라의 新 성장 동력으로 자리매김 할 것으로 판단됨

○ 조만간 상용화가 예측되는 양자컴퓨터를 암호 해독에 사용 시, 이를 대비한 장기간 보안성을 보장하는 새로운 암호 체계 구축이 필요

– RSA (Rivest, Shamir, Adleman) 암호시스템 등 정수론적 난제 기반의 공개키 암호 알고리즘은 현대 컴퓨터의 연산능력 한계를 이용하여 구상된 이후 암호 관련 산업의 비약적 발전 주도함. 반면 최근 양자컴퓨터 등장으로 정수론적 난제 기반의 공개키 암호 시스템은 Shor 알고리즘에 의한 공격으로 무용지물이 될 우려가 대단히 높은 실정임. 향후

30년간 지속 가능한 암호 솔루션은 기존과는 완전히 다른 개념에서 접근해야 하며, 장기적으로는 국가경쟁력 향상에도 긍정적 효과를 기대할 수 있음

- 전술한 바와 같은 암호학적 대변동에 선제적으로 대비하기 위해 미국을 중심으로 CATACRYPT 등 관련 국제학회도 활발히 운영 중인 반면, 우리나라에서는 포스트 양자 암호 분야가 아직은 주목받지 못한 채 관련 연구도 활발히 진행되지 않는 실정임. 이에 정보보안 분야에서 포스트 양자 암호 등 미개척 분야를 중점적으로 발전시켜 안정적인 알고리즘을 개발한 후 안전 분야 통신 시스템에 적용한다면 진일보한 솔루션 구축이 가능할 것임

○ 재난망 구축 시 안전한 보안 솔루션 도입 절실

- 미래부·국민안전처 공동으로 2014년 7월 재난망을 PS-LTE (Public Safety-Long Term Evolution) 방식으로 개발하기로 결정, 정보화전략계획(ISP) 수립 연구 중[1]인데 LTE 방식을 재난망에 적용 시 보안취약점에 대해 연구된 자료가 매우 부족할 뿐 아니라 해결해야 할 보안 문제가 산적해 있음
- 핵심 보안요구기능인 '유·무선 구간 암호화'의 경우, 전술한 포스트 양자 암호 기술을 개발·적용한다면 최고의 보안성을 확보할 수 있고 수십 년간 활용할 수 있는 재난통신망을 구축할 수 있음

○ 다양한 영역으로 적용 확대 등 新 산업 소요 창출

- 미래부 추산 약 2조 ~ 5조 원이 소요되는 재난통신망이 성공적으로 구축될 경우, 관련된 안전 및 보안 산업 발전에 촉매 역할을 수행할 것으로 기대되며, 재난통신망 관련 기관에서 요구하는 보안 수준을 충족한다면 해당 기관에서 추진하는 새로운 통신망 보안 산업 수요도 창출할 수 있음
- 상기 기술은 보안을 가장 기본적으로 구비해야 하는 국방 분야 통신 등에 활용되어 민·군 공용 기술이 될 가능성도 대단히 높고, 기밀 통신 패러다임을 획기적으로 변경함으로 인해 산업계 측면에서는 관련 산업의 비약적인 성장을 견인할 수 있을 것으로 예상됨. 또한, 정보보안 산업이 한 가지 영역에만 국한되지 않고 수요자 요구사항에 부합하게 특성을 조정하여 범용으로 활용할 수 있어야 산업 발전을 선도할 수 있음

■ **연구 범위**

○ 재난통신망(PS–LTE) 보안 취약점 분석 및 대응 방안 연구

– 선진국의 재난망 구축 사례 조사

– 보안 취약점 해결 방안 연구

○ 장기간 보안성을 보장하는 방안 제안

– 30년 이상의 보안성을 보장할 수 있는 신규 암호 체계 연구

– 신규 암호 체계를 이용한 인증 및 개인 식별 방안 연구

○ 단대단 암호가 요구되는 국방용 재난망 적용 시 파생 전략 산업 발굴

– 기존 보안 패러다임에 국한되지 않으면서도 지속 성장 가능한 전략 산업 제시

○ 참여 연구자는 연구책임자 외 7명

〈참여 연구진 소개〉

구 분	소속/직위/성명	담당 역할
연구 책임	카이스트/정교수/김광조	– 연구과제 기획, 조정, 관리
연구 참여	카이스트/박사과정/최락용	– 양자보안 산업 연구
	카이스트/석사과정/정제성	– 국가재난망 구축, 사물인터넷 보안 산업 연구
	카이스트/석사과정/김학주	– 생체모방 보안 및 신경망 암호 산업 연구
	카이스트/석사과정/김경민	– 드론/로봇 보안 산업 연구
	카이스트/석사과정/박준정	– 국내 정보보호 산업 동향 조사
	카이스트/석사과정/안수현	– 국가재난망 추진 현황과 문제점 조사
	카이스트/석사과정/홍진아	– 드론/로봇 보안 산업 연구

2

국가재난망의 추진 현황과 문제점

서해 훼리호 침몰(1993년), 삼풍백화점 붕괴(1995년), 대구지하철 방화사고(2003년), 세월호 침몰(2014년)과 같은 대형 공공안전재난 사건은 재난을 막기 위한 통신망의 필요성을 인식시켰고, 이러한 필요성에 대응하여 경찰, 소방, 해경, 지자체, 공군이 통신망을 운영하고 있음. 아래에 경찰, 소방, 해경, 지자체, 공군에서 어떤 통신망을 사용하고 어떠한 용도로 사용하는지 나타내었음

■ **경찰**

○ TETRA (TErrestrial Trunked RAdio), VHF/UHF

– 재난 시는 통합지휘망으로 활용하고 평상시에는 치안 용도로 사용

■ **소방**

○ TETRA (TErrestrial Trunked RAdio), VHF/UHF

– 소방행정지휘 및 소방작전에 사용

■ **해경**

○ iDEN, VHF/UHF

– 해상안전관리 및 업무연락으로 사용

■ **지자체**

○ VHF/UHF

– 산불예방용 무선통신망은 시·군 단위로 운영

■ **공군**

○ Wibro

– 정비업무(정비데이터 기록·입력)에 사용

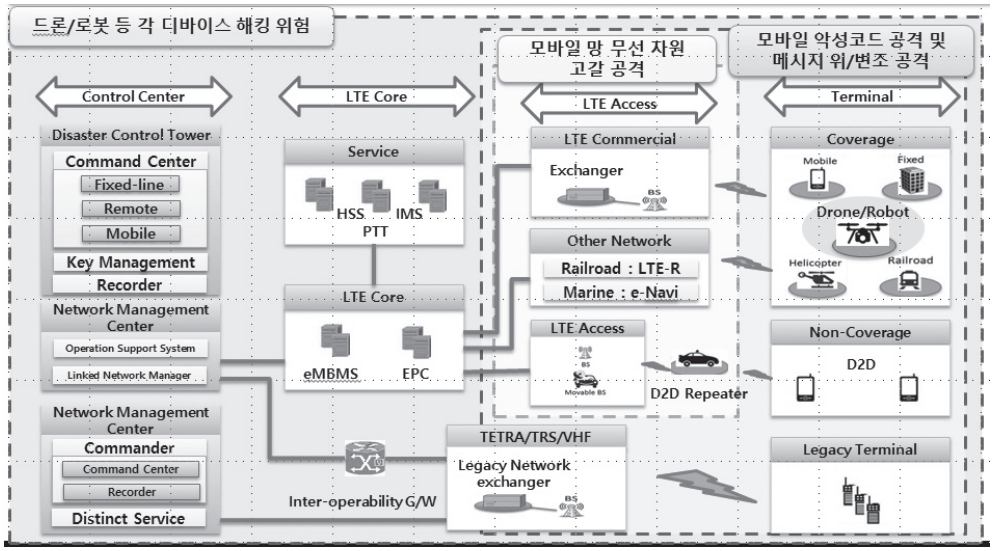
이와 같이 통신망을 운영함으로써 대형 공공안전재난에 대비하였지만, 이에 대한 문제점 또한 발생하고 있음. 대표적으로 위에서 볼 수 있듯이 모두 같은 통신망을 사용하는 것이 아닌 소방·경찰·지자체 등이 다른 기술방식의 통신망을 별도로 운영하고 있어 재난 발생 시 기관 간 협업에 어려움이 있음. 뿐만 아니라 위 통신망에서 가장 많이 사용되는 TETRA, VHF/UHF 또한 자체적으로 문제점을 가지고 있음.

VHF/UHF의 경우 멀티미디어 서비스가 불가능하고, 할당 주파수폭이 작아 충분한 채널 확보가 곤란하여 통신이 되지 않는 음영지역이 많으며, TETRA의 경우 서울·경기 통합지휘무선통신망과 6대 광역시 고속도로 주변에 경찰망이 운영 중이나, 일부 지하구간 불통 및 데이터 통신이 곤란한 상황이며, 유럽전기통신표준협회(ETSI)가 정한 표준이므로 이에 대한 비용을 지불해야 하는 문제 또한 존재하는 상황임. 이러한 문제점을 해결하기 위해, 소방·경찰·지자체 등이 공용으로 사용할 수 있는 국가재난망이 필요하게 되었고, 이는 PS-LTE라는 기술을 사용하는 국가재난망의 탄생으로 나타나게 되었음.

PS-LTE를 사용하는 국가재난망은 서비스 지역을 확대시키며, 기존의 통신망에서 제한되었던 음성·영상 등 다양한 멀티미디어를 전송가능하게 함. 또한 통합으로 운용되므로 기존의 서로 단절되었던 통신망이 하나로 연결되어 양방향으로 협력적인 의사소통이 가능하게 되어 대형 공공안전재난 사건에 아주 유용하게 사용될 것으로 기대됨. 하지만 이러한 편의성에도 불구하고 PS-LTE망에서 보안 문제가 제기되고 있음.

PS-LTE는 기존의 네트워크에서 발생하던 여러 가지 공격들이 가능한데, 대표적으로 단말 대 단말 통신에서 비정상 트래픽이 유입되는 공격, 무선 자원 고갈 공격, IP 스푸핑을 악용한 비정상 트래픽 유입 공격, 모바일 악성코드 공격, SIP 메시지 위/변조 공격 등 다양한 보안 위협들이 존재하는 상황임. 〈그림 1〉은 위에 제시한 공격들이 어느 부분에서 나타날 수 있는지 나타내고 있음. 제시된 보안 위협 중 하나라도 성공한다면 실제 대형 공공안전재난 사건 발생 시 통신 불능을 만들거나 실제 대형 공공안전재난 사건이 발생하지 않는 상황에서도 통신을 불가능하게 만들어 더 큰 피해를 야기시킬 수 있음.

〈그림 1〉 PS-LTE 보안 위협



3

국가재난망 구축[2]

■ **목표**

○ 국가재난안전통신망은 통화폭주 등 극한 상황 및 재난 시 신속한 초기 대응을 위하여 〈표 1〉의 형태로 음성, 데이터, 영상 정보를 원활하게 송수신하는 통신망 구축을 목표로 함

〈표 1〉 국가재난안전통신망 발전 전망

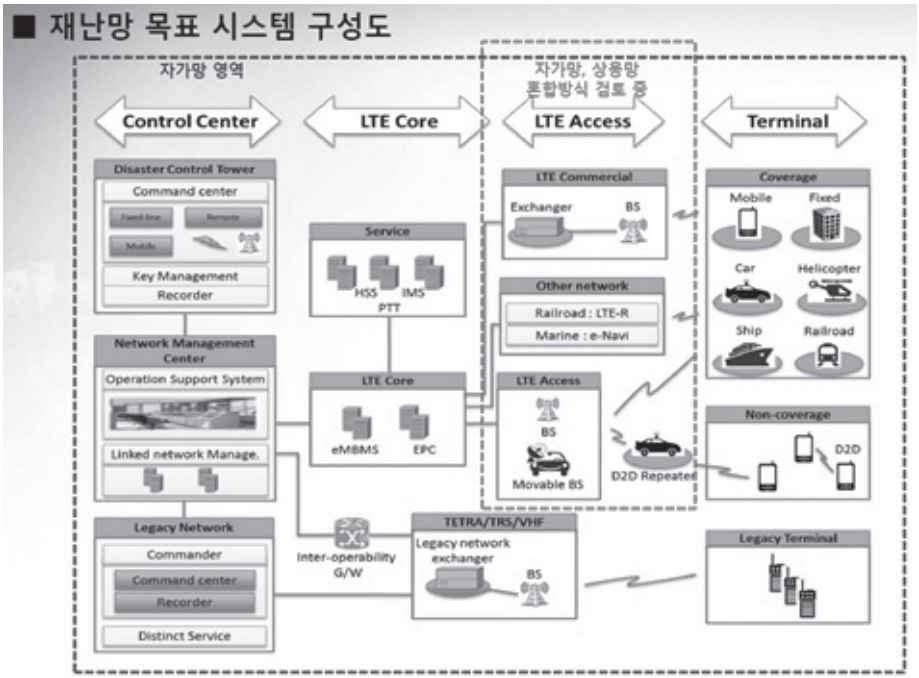
As-is		To-BE
협대역/서비스 지역제한	⇒ 재난 환경변화	광대역/서비스 지역 확대
음성 중심		음성·영상 등 다양한 멀티미디어
재난발생 시 활용	대형화	재난발생 및 평시(예방) 활용
기관별 구축운용	복잡화	통합 구축·운용
단방향/단일기관 의사소통	다양화	양방향/협력적 의사 소통

■ **구축방식 검토 결과**

○ 〈그림 2〉와 같이 국가재난안전통신망 코어부문은 자가망으로 구축하되, 상용망을 활용

하여 커버리지를 확보하며, 음영지역은 이동기지국을 통해 해소하는 방식이 적절할 것으로 보임. 또한 커버리지 확보 우선순위는 인구밀집지역, 대도시, 상용망 커버리지 미확보 지역과 철도, 해상 등 통합망 구축으로 주파수 이용 효율의 극대화가 가능한 점을 고려, 재난망 이용 소요 제기 부처를 수용하여 운영하기를 권장함

〈그림 2〉 재난망 목표 시스템 구성도



〈출처: 조학수, 2015 재난안전통신망 보안이슈 및 해결방안〉

4

국내 정보보호 산업 동향

■ **정보보호 산업의 정의**

○ 초연결사회가 도래함에 따라 사물인터넷(IoT)이 미래의 새로운 경제성장 동력으로 부상하고 있는 가운데 향후 우리나라의 미래를 좌우할 최첨단 기술집약적 산업

○ 암호·인증·인식·감시 등의 보안기술이 적용된 제품을 제조 또는 판매하거나, 보안기술 및 보안제품을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하기 위한 모든 서비스 제공과 관련되는 산업

■ **정보보호 산업의 특성 및 문제점**

○ 정보보호 산업은 성장발전 가능성이 높은 신성장 산업이며, 국가의 안보와 관련된 방위산업으로 정보보호 산업의 범위는 〈그림 3〉과 같음. 또한, 차세대 고부가가치를 보유한 미래지향적인 산업임

○ 그러나 현재까지는 각종 정보통신 공격으로부터 통일적·체계적으로 대응을 하고 있지 못하며 산업 역시 선진국에 비해 낙후된 상황임

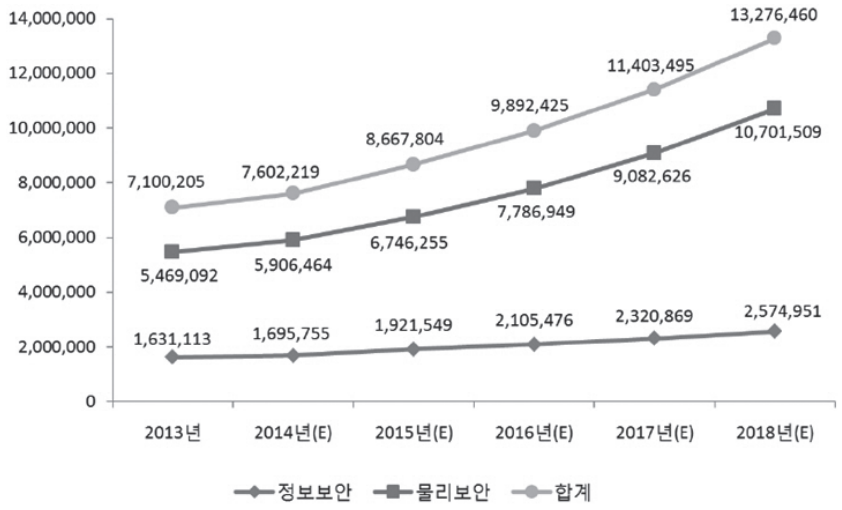
〈그림 3〉 정보보호 산업 범위

〈출처: 2014 국내 정보보호산업 실태조사, KISIA〉

■ **국내 정보보호 산업 매출 전망**

○ 〈그림 4〉와 같이 국내 정보보호 산업은 매년 발전[3]하고 있지만, 그 성장세가 둔화되고 있음을 통계자료를 통해 확인할 수 있음. 정부에서는 2012년을 기준으로 향후 연간 연평균 성장률을 12.48%로 예상하였으나, 2014년에는 향후 5년간 연평균 성장률이 9.6%로 줄어들 것으로 분석하였음

〈그림 4〉 국내 정보보호 산업 매출 현황 및 전망



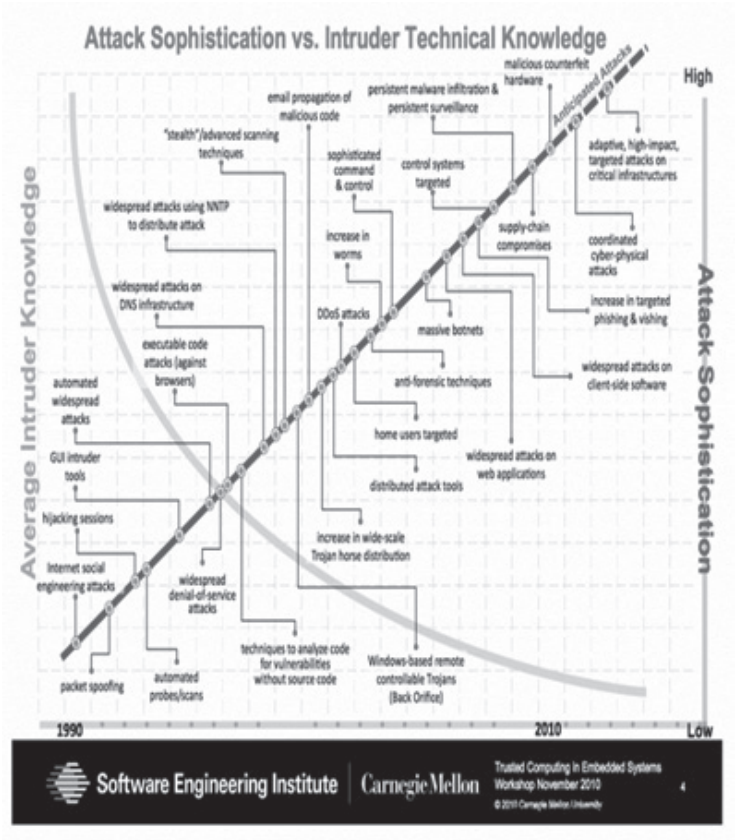
〈출처: 2014 국내 정보보호산업 실태조사, KISIA〉

○ 미래창조과학부는 2019년까지 시장 규모를 100% 확대하고 수출액을 3배 증대시키는 한편, 전문인력을 적극 양성한다는 청사진을 제시[4]하였지만, 장기간 보안성을 보장하면서도 미래 성장 동력이 되는 산업을 발굴하는 것은 다소 미흡한 실정임

■ **보안 위협과 기술 변화**

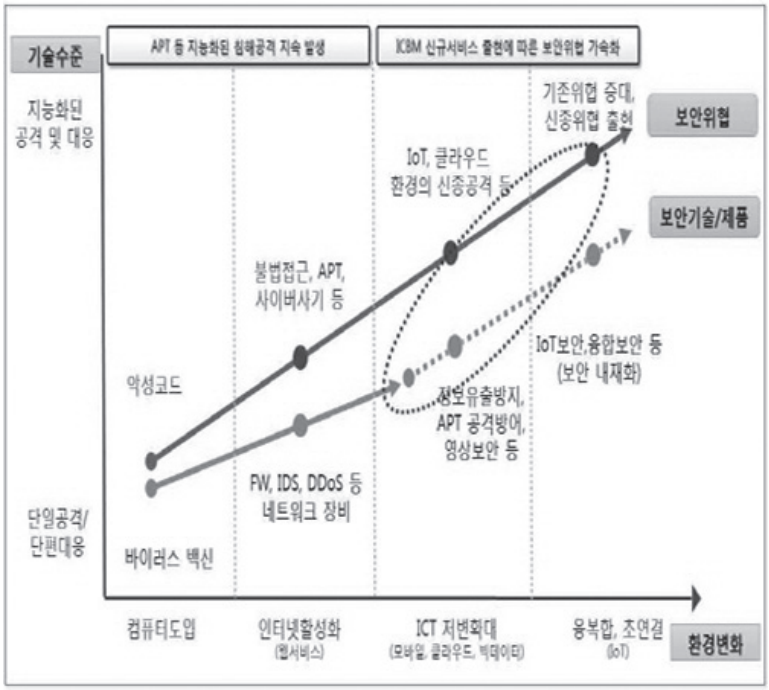
○ 미국 카네기멜론대학교 소프트웨어 엔지니어링 연구소에서는 〈그림 5〉와 같이 시대별 공격 고도화 수준과 지식 변화 추세를 분석하여 과거에 비해 현재, 그리고 미래 해커의 지식은 점차 낮아지지만, 공격 고도화 수준은 계속 높아질 것으로 예측하고 있음

〈그림 5〉 시대별 공격 고도화 수준과 공격자의 지식 변화 추세



○ 우리 정부에서도 보안 환경 변화에 따라 보안 위협은 지속적으로 증가하고 있으며, 그 증가 속도를 보안기술/제품이 따라가지 못하는 것으로 분석하고 있음. 따라서 보안 위협과 보안 기술 사이의 갭은 시간이 지날수록 커지고 있는 추세임

〈그림 6〉 보안위협과 보안기술의 관계[4]



■ 국내외 정보보호 기술 수준 현황

○ 〈그림 7〉에 각 보안 분야별 선진국에 대비한 우리나라의 기술 수준을 나타냄. 정보보호 분야에서 미국이 최고 수준의 원천기술을 보유하고 있으며, 우리나라는 미국 대비 79.9% 기술 수준으로 1.6년의 기술 격차가 있음[5]. 물론 시장이 협소한 일부 제품에서는 세계 수준에 근접해 있기도 하지만, 보안 주요 분야 원천기술은 부족한 실정임. 이 차이가 더 커질 경우 선진국 기술에 완전 종속될 우려가 있기 때문에 미래 신성장 동력을 개척하여 선진국을 빠르게 추격해야 정보보호 분야에서 '추격자(fast follower)'가 될 수 있음

〈그림 7〉 보안 분야별 선진국 대비 우리나라 기술[5]

5

중장기 전략 사업 후보

1) 중기(10~15년) 산업군

■ **사물인터넷(IoT) 보안 산업**

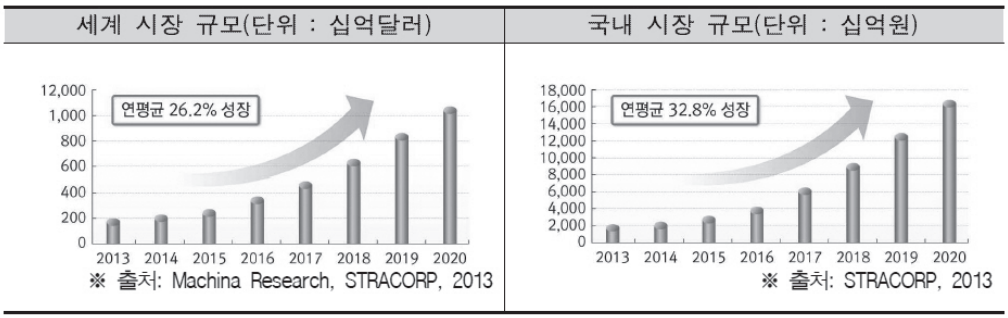
○ 정의

– 사물인터넷은 생활 속 사물을 유무선 네트워크로 연결해 정보를 공유하는 것으로 이와 관련된 보안 산업을 말함. 이는 디바이스, 네트워크, 플랫폼/서비스로 구분됨

○ 국내외 동향

– 〈그림 8〉은 IoT 보안 산업의 시장 전망을 나타낸 그림으로 국내는 '13년 2.3조 원→'20년 17.1조 원, 연평균 32.8% 성장 전망되며, 국외는 13년 2천억 달러 → 20년 1조 달러, 연평균 26.21% 성장 전망됨. 또한 전 세계 사물인터넷 응용SW와 서비스의 시장성장률(~'20년)은 각각 89%와 122%로, 사물인터넷 기기(11.2%)에 비해 응용SW, 서비스 중심으로 성장할 것으로 예상됨

〈그림 8〉 2020년까지의 시장 전망[6]



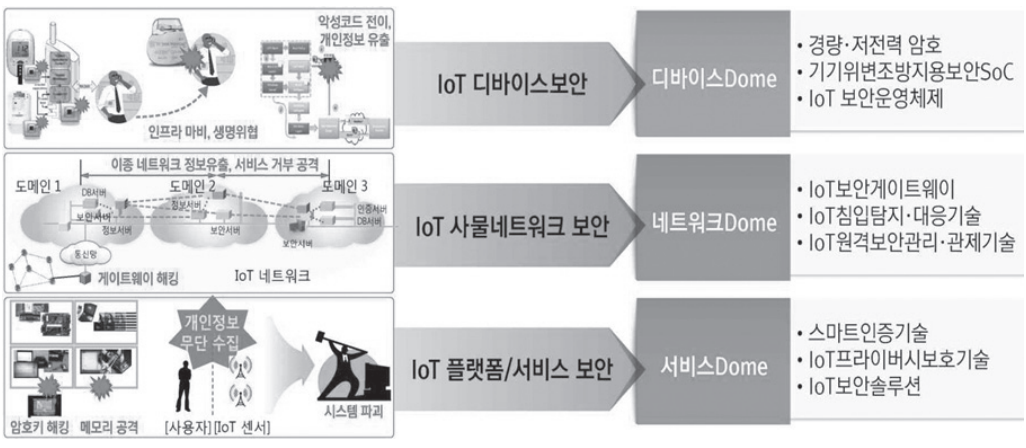
○ 문제점

– 각종 해킹을 통하여 개인정보 유출, 산업 시스템 피해 등이 발생할 수 있음

○ 사물 인터넷 안전 요구사항

– IoT 제품·서비스를 안전하게 보호하기 위해서는 〈그림 9〉와 같이 3계층(디바이스, 네트워크, 서비스/플랫폼) 9대 핵심 원천기술 개발이 필요할 것으로 보임

〈그림 9〉 9대 IoT 보안 핵심기술 개발(시큐어 Dome)[6]



○ 응용분야

– 향후 10년에는 〈그림 10〉과 같이 스마트홈 보안을 위해 스마트홈/가전 기기 출시 전 보안 취약점 점검 및 지속적 보안패치 적용을 할 수 있으며 헬스케어 시스템에서 개인정보, 질병정보를 저장·처리하는 의료장비 및 이와 연동되는 데이터 처리장치 프라이버시 보호를 위한 인증 및 암호화 기능이 적용될 것으로 보임. 또한 자동차 보안 분야에서는 ABS (Automatic Break System), TPMS (Tire Pressure Monitoring System) 등 자동차 주행 및 구동장치의 중단/오작동을 방지하기 위한 보안기능(데이터 암호화·복구, 비인가 접근통제 등)이 적용될 것임

〈그림 10〉 IoT 보안 산업의 응용분야

○ 산업전망

– 사물인터넷 산업은 위치추적 시스템을 통한 사물 및 사람 추적, 주문관리, 물류 추적 산업 등과 차량제어, 자동비상콜, 차량도난방지, 고속버스 차량관제사업 등과 관련된 교통 관련 산업이 발전할 것으로 보이며 또한 혈압, 당뇨 등 개인건강 체크솔루션 등의 헬스케어 분야도 크게 발전할 것으로 예상됨

○ 국가 차원의 미래 전략

– 사물인터넷 국가전략을 수립하여 공공기관 및 민간기업에 적절한 가이드를 제시함으로써, 스마트시티, 스마트 인프라 등 지속적인 혁신기술 개발 및 세계 주도적 역할을 추구해야 함. 또한 경제성장뿐만 아니라 농업, 교육, 에너지, 헬스케어, 공공안전, 보안 및 교통 등 일상생활에서의 소비자 권한 강화를 강조하고, 기업의 물류관리 간소화 및 공급망 비용 절감 등에 따른 이익을 소비자에게도 분배할 수 있도록 해야 함. 또한 관련 법률 및

정책을 지속적으로 개발하여 사물인터넷이 현실에 사용되는 데 제한이 없도록 해야 함

■ 드론/로봇 보안 산업

○ 정의

– 로봇이란 컴퓨터 프로그램에 의해 입력된 행동을 하는 기계 혹은 소프트웨어를 통칭하는 것을 말하며 〈그림 11〉과 같이 산업용 로봇, 지능형 로봇, 안드로이드 등으로 구분됨. 드론은 로봇의 일종으로, 무인 항공기(Unmanned Aerial Vehicle, 이하 UAV)를 지칭함. UAV는 조종사가 탑승하지 않고 지정된 임무를 수행할 수 있게 제작된 비행체를 말함

– 드론/로봇 보안 산업이란 점차 대중화되고 있는 드론/로봇의 기밀성·무결성·가용성 등 보안 요구 사항을 보장하기 위한 제품을 생산하거나, 관련 보안 기술을 활용해 드론/로봇을 이용한 범죄 등을 방지하는 산업을 말함

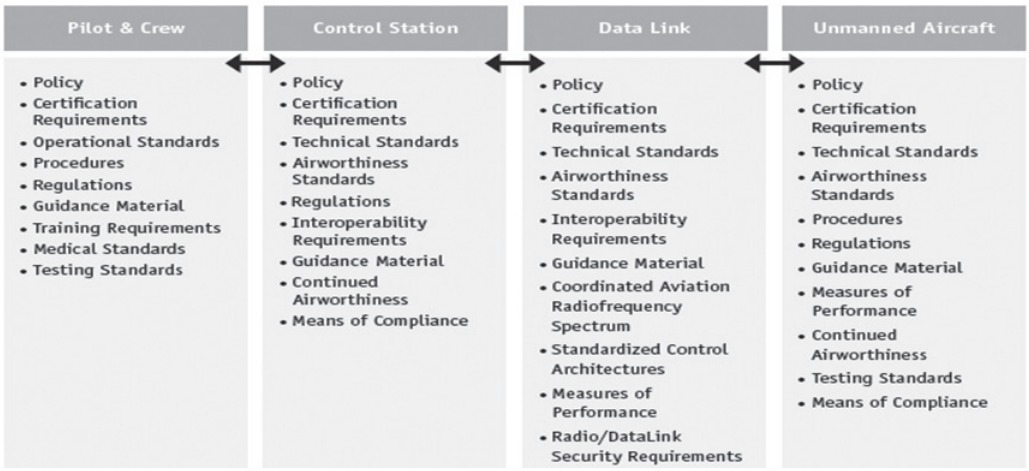
〈그림 11〉 로봇의 예

○ 문제점

– 실제 드론의 자이로센서를 해킹하여 비행하고 있는 드론을 추락시키는 등 각종 해킹을 통한 기능 이상, 사생활 침해, 강제 탈취 및 변조의 위험성 문제 등이 발생할 수 있음

○ 드론/로봇 안전 요구 사항

〈그림 12〉 드론/로봇의 안전 요구 사항



〈출처: 미국연방항공청[Federal Aviation Administration, FAA], 2013 Integration of Civil Unmanned Aircraft Systems in the National Airspace System Roadmap, 2013〉

– 〈그림 12〉와 같이 드론/로봇의 보안을 위해서는 드론/로봇을 조종하는 파일럿, 컨트롤센터, 드론/로봇 사이에서의 데이터 링크, 드론/로봇 기기 자체에서의 안전 등 다양한 측면의 요구 사항이 존재함

○ 국내외 동향

– 〈그림 13〉은 로봇 시장의 규모를 예측한 것으로 국내에서의 드론 시장은 2013년 9천만 달러에서 2022년 5억 2500만 달러로 연평균 22% 성장이 기대되고, 로봇 시장은 2008년 3천억 원에서 2020년 100조 원으로 연평균 62.2%의 성장이 기대됨

– 〈그림 14〉는 드론 시장의 규모를 예측한 것으로 해외의 경우 드론 시장은 2013년 60억 달러 규모에서 2023년 114억 달러로 연평균 6.6% 성장이 기대되고, 로봇 시장은 2008년 200억 달러 규모에서 2020년 5천억 달러 규모로 연평균 30.7% 성장이 기대됨[7]

– 국내와 해외 모두 드론/로봇 시장이 폭발적으로 성장할 것으로 예측되는 가운데, 드론/로봇 보안에 관한 연구는 현재 로드맵 등이 논의되는 단계로, 상대적으로 실제 연구개발 결과가 미흡함

〈그림 13〉 세계 및 국내 로봇 시장 규모[7]

구 분		현재시장규모	예상 시장규모	
			2010년	2020년
세계 시장규모(억 불)		200	1,500	5,000
한국시장 규모 (억 원)	산업용 로봇	2,700	40,000	400,000
	비제조용 서비스 로봇	300	60,000	600,000
	계	3,000	100,000	1,000,000

〈그림 14〉 세계 및 국내 드론 시장규모

〈출처: 이투데이〉

○ 응용분야

– 향후 10년간 그동안 연구된 실제 드론/로봇 해킹 사례를 바탕으로 하여 〈그림 15〉와 같이 드론/로봇의 취약점 보완, 드론/로봇의 안전성/신뢰성 보장을 위한 키관리/키분배 프레임워크 개발, 드론/로봇 강제 탈취 및 변조 방지를 위한 인증 및 암호화 기능 적용, 드론/로봇 간 네트워크 통신 보안 등의 산업이 발전할 것으로 기대됨

〈그림 15〉 드론/로봇 보안 산업 응용 분야

○ 산업 전망

- 전 세계적으로 로봇 시장은 2008년에서 2023년까지 연평균 30.7%의 성장률로 총 5천억 달러의 시장을 형성할 것으로 기대됨. 이 데이터를 바탕으로 2025년에는 최소 8천 5백억 달러의 시장을 형성할 것으로 추측됨
- 드론/로봇 보안은 현재 로드맵 논의 단계에 있기 때문에 정확한 시장 예측은 존재하지 않음. 세계 IT 시장 규모(2014년 4552조 원) 대비 세계 정보보호 시장 규모(2014년 209조 원)를 드론/로봇 보안 시장 규모 측정에 적용[8]한다면, 2025년경 드론/로봇 보안 산업은 약 390억 달러의 시장을 형성할 것으로 추측됨

○ 국가 차원의 미래 전략

- 로봇 보안 프레임워크에 관한 연구는 ETRI 등에 의해 수행된 바가 있음[8]. 또한 지식경제부의 2010년 IT R&D 발전 전략에서 융합 보안의 하위 분야로 로봇 보안이 포함되어 있음[7]
- 하지만 드론/로봇의 여러 가지 안전 요구 조건에 비해 로봇 보안의 목표로 설정된 기술은 네트워크로봇 보안, 로봇간 통신 보안 등[7] 한정되어 있음. 따라서 안전한 드론/로봇을 보장하기 위해 드론/로봇 보안에 대한 전 방위적 연구가 이루어져야 함
- 드론/로봇의 부분을 이루고 있는 기술/부품 등의 해킹, 네트워크 공격, 탈취 및 변조, Zero-day 공격 등에 대해 보안 산업 개발을 진행, 최종적으로는 국제적으로 경쟁력을 갖춘 드론/로봇 보안 기업 양성을 목표로 함

2) 장기(30년~) 산업군

■ 양자보안 산업

○ 정의

– 양자보안이란 해킹 등 보안위협을 해결할 수 있는 가장 강력한 대안으로 양자현상에 기초한 양자키분배(Quantum Key Distribution, 이하 QKD) 네트워크를 설계하거나 양자컴퓨터를 이용한 공격에 내성을 가지는 포스트양자암호(Post Quantum Cryptography, 이하 PQC) 등의 보안기술이 있음

– 양자보안 산업이란 QKD 네트워크, PQC 등의 양자보안 기술이 적용된 제품을 생산하거나 관련 보안기술을 활용하여 재난, 재해, 범죄 등을 방지하는 서비스를 제공하는 기술을 말함

○ 국내외 동향[9]

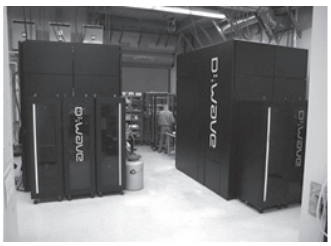
– 국내에서는 SKT, ETRI 등에 의해 QKD 네트워크에 대한 연구가 진행되었으며 2014년 SKT에 의해 〈그림 16〉과 같은 국내 첫 QKD 네트워크 기기가 출시됨

– 해외의 경우 미국, 유럽, 일본, 중국 등 주요 국가에서 QKD 네트워크 테스트 베드가 구축되었으며 ETSI 주관 하에 QKD 표준화 작업이 진행되고 있음

– 〈그림 17〉과 같이 캐나다 D-wave사에 의해 세계 최초 양자컴퓨터가 개발되었으며, ETSI 주관 하에 Quantum-safe cryptography의 표준화가 초기단계에 있음

– 학계에서는 QKD 네트워크 및 양자암호 관련 학술대회인 QCrypt가 매년 개최되고 있으며, 약 20년 전부터 양자컴퓨터에 안전한 암호 설계 방법을 연구하여 관련 학술대회인 PQCrypto가 정기적으로 개최되고 있음 〈그림 18〉

〈그림 16〉 QKD 네트워크 기기 / 〈그림 17〉 세계 최초 양자컴퓨터 / 〈그림 18〉 양자보안 관련 학술대회



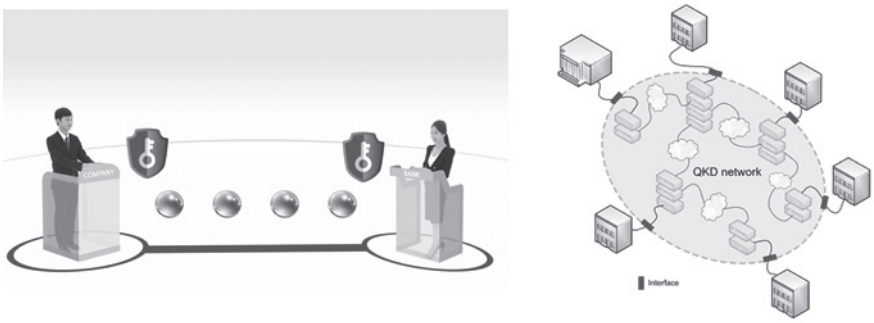
○ 현재 문제점

– 양자보안 산업의 가장 큰 문제는 양자현상에 기초한 QKD 네트워크와 양자컴퓨터 등 플랫폼이 아직 상용화되어 있지 않아 알려지지 않은 보안 위협이 있을 수 있다는 것임

○ 응용 분야

– 향후 10년간은 〈그림 19〉와 같이 그동안 진행된 QKD 네트워크에 대한 연구를 기반으로 QKD 네트워크 구축 및 상용화 산업, QKD 네트워크를 이용한 SCADA 시스템 구축 산업, QKD 네트워크를 이용한 국가재난안전통신망 구축 산업 등을 할 수 있을 것으로 기대됨

〈그림 19〉 QKD 네트워크의 활용 예



– 향후 30년의 경우 〈그림 20〉에서처럼 QKD 네트워크를 이용한 응용 어플리케이션으로 회사 자료 보안 백업 서비스 산업 등이 가능하며, PQC를 이용하여 end-to-end 보안을 위한 PQC 기반 암호화 및 인증 소프트웨어 개발 산업을 할 수 있을 것으로 예상됨. 이를 응용하여 헬스케어 기기 및 클라우드 컴퓨팅 보안 산업, 인터넷뱅킹 및 모바일뱅킹 보안 산업, 자동차 스마트 키의 PQC 기반 페어링을 통한 자동차보안 산업 등을 진행할 수 있을 것으로 기대됨

〈그림 20〉 양자보안 산업의 응용 분야

○ 산업 전망

– 시장조사업체 MRM에 의하면 QKD 네트워크 산업이 2015년에서 2020년까지 연간 10.4%의 성장률로 총 30조 원의 시장을 형성할 것으로 전망하였으며, 이 데이터를 바탕으로 2040년경에는 PQC 산업이 추가되어 최소 80조 원 이상의 시장을 형성할 것으로 추측하고 있음

○ 국가 차원의 미래 전략

– QKD 분야는 이미 미래부에 의해 추진전략이 세워져 활발한 투자가 이루어졌으며 ETRI, SKT 등에 의해 연구가 진행되고 상용화를 위한 연구 또한 활발하게 진행 중에 있음

– 반면 PQC 분야의 경우 미국, 유럽 등에 비교하여 우리나라는 PQC 분야의 초기 연구 단계에 있으며 이 분야에서 '추격자(fast follower)'가 되기 위해 미래부 차원에서 빠르게 전략적 투자가 진행되어야 함

– PQC 기술 등 양자보안 기술을 이용하여 양자컴퓨터 공격, Zero-day 공격 등에 대해 절대적 안전성을 제공하는 보안 산업 개발을 진행, 최종적으로는 국제적 보안 기업인 RSA Corporation과 유사한 양자보안 기반 기업 양성을 목표로 함

■ 생체모방 보안 산업

○ 정의

– 생체모방 보안(Bio-inspired Security) 산업은 생체를 모방한 알고리즘을 다양한 정보보호 분야에 접목하여 System Scalability 유지, Unknown Attack 탐지 등 기존 보안 문

제들을 해결할 수 있는 산업으로 정의됨. 특히 수동적이고 공격에 반응하는 형태를 가진 기존 보안 제품들에 비해 능동적이고 proactive한 방어제로 적용 가능하다는 장점을 가지고 있음. 생체를 모방한 알고리즘은 각종 생물체의 행태, 군집 형태, 세포 기전 등을 접목하여 머신 러닝 등의 분야에서 연구되고 있는 알고리즘을 의미함. 생체모방 알고리즘에는 인공신경망(Artificial Neural Network) 알고리즘, 군집지능(Swarm Intelligence) 알고리즘, Genetic 알고리즘 등이 있음

○ 국내외 동향

– 국내에서는 생체모방 알고리즘을 사용하여 무선메시망(Wireless Mesh Network) 라우팅 성능 향상 등의 분야에서 집중적인 연구가 이루어지고 있음. 보안에 관련해서는 생체모방 알고리즘을 활용한 네트워크 침입 탐지 시스템의 초기 연구가 진행 중이나 정보보안 분야 전반에 걸쳐 다양하고 집중적인 연구가 부족한 상황임

– 국외에서는 인공면역체계(Artificial Immune System) 알고리즘을 활용한 안티바이러스 초기 연구 및 다양한 생체모방 알고리즘을 활용한 네트워크 침입탐지 시스템에 대한 초기 연구가 이루어지고 있음. 국내에 비해 다양하고 집중적인 연구 시도가 진행 중임

○ 현재 문제점

– 전반적으로 생체모방 보안 분야는 현재 연구 초기 단계로서 기존 보안 문제들의 해결 가능성이 확인된 상태임. 생체모방 보안 분야는 지구상에 존재하는 생체의 종류와 적용 가능한 응용 보안 분야가 방대하여 다양하고 지속적인 연구가 필요함. 융합 보안 특성상 생명공학과 정보보안 학계 간 지속적인 공동 연구가 필수적이나 아직 활발히 이루어지고 있지 않음. 현재 System Scalability의 보장 연구에 큰 진전이 있었으나 알고리즘 Training 시간의 최적화 연구가 추가로 필요함. 또한 현재까지 연구된 Unknown Attack의 탐지율과 오탐률이 산업에 적용되기에는 부족하다는 단점을 가지고 있음

○ 응용 분야

– 〈그림 21〉에서 보듯 향후 10년에는 현재 집중적인 연구가 이루어지고 있는 안티바이러스와 네트워크 침입탐지 시스템에 생체모방 보안이 적용될 것으로 보임. 기존에 널리 쓰이고 있는 Signature 기반 제품들을 완전히 대체하기보다는 proactive한 생체모방 알고리즘의 장점을 기존 방식과 융합시키는 방향으로 진행될 것으로 판단됨

– 향후 30년에는 생체모방 알고리즘을 주도적으로 사용하는 안티바이러스 및 네트워크 침입탐지 시스템이 개발될 것으로 예측됨. 또한 암호시스템 설계 및 해독, 사용자 및 기기 인증, CCTV 관제 시스템을 포함한 물리적 보안 산업에도 생체모방 알고리즘이 접목 및 활용될 것으로 판단됨

〈그림 21〉 생체모방 보안 산업의 응용 분야

○ 산업 전망

– 현재로서는 생체모방 알고리즘과 기존 정보보호 산업의 융합이 아직 불완전하여 체계적인 산업 전망이 어려움. 관련 연구가 지속적으로 이루어지면서, 기존 정보보호 산업에 대한 보완재의 역할을 수행할 것으로 전망됨. 새로운 미래 산업 창출의 여부는 생체모방 알고리즘의 연구 성과에 달린 실정임

○ 국가 차원의 미래전략

– 생체모방 보안 산업은 현재 초기 연구 상태이지만 미래에 기존 정보보안 산업의 보완재 및 대체재가 될 가능성을 충분히 보여주고 있음. 분야의 방대함에 비해 국내에서는 제한된 초기 연구만이 이루어지고 있는 상황이므로, 국가 차원에서 지속적인 연구 지원을 통해 연구 및 시장 형성의 주도적 역할을 선점하는 것이 바람직함. 그러므로 생명공학과 정보보안 학계의 다양한 공동연구 프로젝트를 꾸준히 지원하는 것이 중요함

■ **신경망 암호 산업**

○ 정의

– 신경망 암호 산업은 새로운 암호학인 신경망 암호학(Neural Cryptology)을 통해 정보보

안의 가장 기초에 해당되는 암호시스템의 설계 및 해독을 하는 산업임. 신경망 암호학에서 대표적으로 사용되는 인공신경망(Artificial Neural Network) 알고리즘은 인간의 뇌 신경망의 상호작용을 모방하여 일반적인 프로그래밍을 통해 풀기 힘든 문제의 해답을 찾는 알고리즘의 한 예임. 신경망 암호학은 인공신경망을 암복호화에 활용하는 암호시스템 설계 분야, 암호와 같은 Stochastic한 알고리즘 분석 및 해독 분야, 그리고 보안통신이 필요한 양자 간의 동기화에 사용되는 암호키 교환 프로토콜 분야로 나뉨

○ 국내외 동향

- 국내의 관련 초기 연구는 거의 전무한 실정
- 국외에서는 인공신경망을 암복호화에 활용하는 초기 연구, 기존 암호를 신경망으로 모델링하여 해독하는 초기 연구, 신경망의 상호동기화 특성을 활용한 암호키 교환 알고리즘 연구가 이루어지고 있음. 인공신경망을 활용한 암호시스템 설계 연구의 예로는 Boolean Algebra와 Backpropagation Neural Network를 활용한 공개키 암호시스템 등이 있음. 인공신경망을 활용한 암호시스템 해독은 1995년에 처음 시작되었으며, 현재 암호해독 분야의 새로운 갈래로 다양한 시도가 이루어짐. 인공신경망의 특성을 활용한 암호키 교환 알고리즘은 학계의 많은 관심을 얻어, Tree Parity Machine와 Permutation Parity Machine 등과 같은 알고리즘이 이미 연구 중임

○ 현재 문제점

- 현재 연구 초기 단계로 인공신경망을 활용한 새로운 암호시스템 설계 및 해독 방법의 가능성만 확인된 상태임. 신경망 암호 분야는 체계적이고 집중적인 연구가 지속적으로 필요함

○ 응용 분야

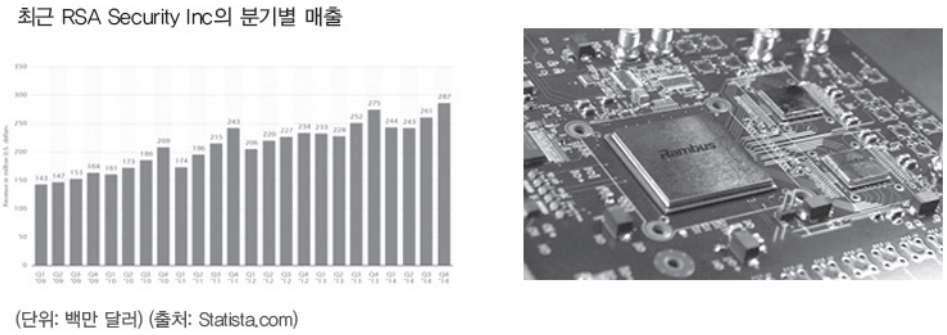
- 인공신경망 연구와 암호시스템 연구의 융합으로 새로운 방식의 암호시스템 설계, 해독, 암호키 교환 메커니즘 등 암호 분야 전반에 걸쳐 응용이 가능함

○ 산업 전망

- 인공신경망을 활용한 암호시스템을 개발하여 그 효용성이 입증되면, 현재 널리 사용되고 있는 공개키 암호인 RSA를 개발하고 RSA를 탑재한 암호시스템의 안전성을 인증해주는 등 분기당 2억 달러 이상의 매출을 올리는 RSA Security Inc.와 같은 기업이 가능함. 또

한 인공신경망을 활용한 새로운 공격방법이 개발되면, 근래 새로 알려진 부채널 공격에 대한 보안성을 인증해주는 회사인 Cryptography Research Inc.와 같은 기업의 설립도 가능함 〈그림 22〉

〈그림 22〉 신경망 암호 산업의 산업 전망



○ 국가 차원의 미래 전략

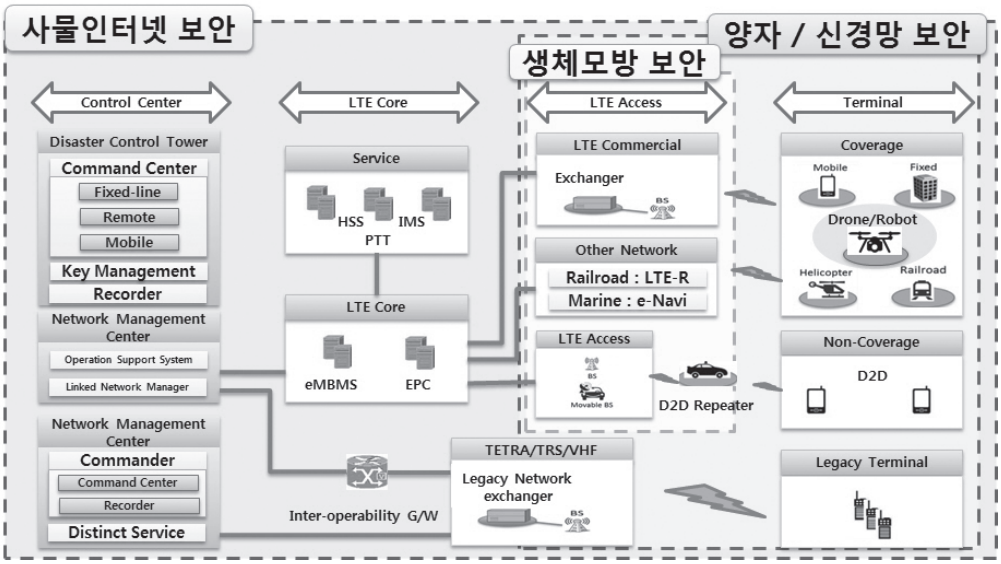
– 신경망 암호 산업은 세계적으로 연구 초기 단계로 새로운 암호시스템에 대한 가능성만 확인된 상태임. 국내에서는 선행연구조차 매우 부족한 실정으로 국가 차원에서 장기적 관점에서 꾸준한 지원이 필요함

6

장기간 안전성을 보장하는 국가재난망 구축

장기간 안정성을 보장하기 위한 국가재난망 보완 적용 방안을 〈그림 23〉에 제시함

〈그림 23〉 국가재난망 보완 적용 방안



7

국가재난망 구축 SWOT 분석

■ **강점**(Strength)

○ 강력한 정부 주도형 안전한 재난망 구축

○ KISIA를 통한 정보보호 산업군이 다양한 정보보안 국내외 사업화 경험 풍부

○ 일부 정보보안 제품 국외시장(미국, 일본 등) 진출

■ **약점**(Weakness)

○ 보안-안전 이질 문화 간 win-win 전략 부재

○ 인공지능 기초 이론 및 양자컴퓨터 이론 전문가 부재로 독창적인 이론 정립이 어려움

○ Firewall, UTM, AV 제품을 제외하고 embedded 보안 제품

■ **기회**(Opportunity)

○ 새로운 융합 보안 산업 기회

○ 융합 보안 고급 인력 양성

○ 정보보안 선진국 도약의 기회

■ **위협**(Threat)

○ 미래 예측이 어려워 장기간 연구 계획 추진 위험

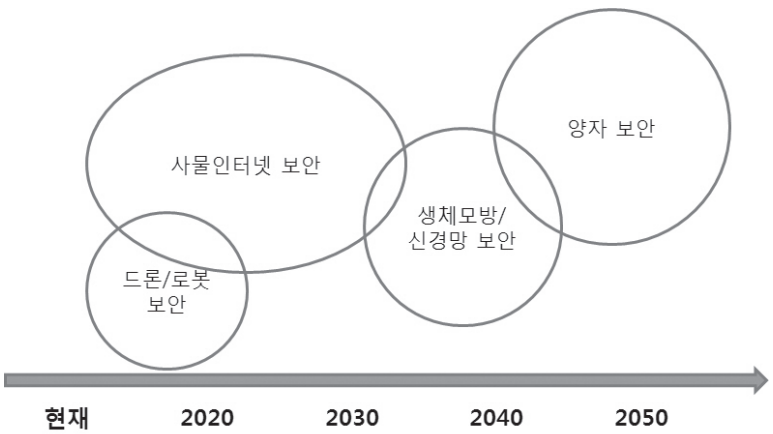
○ 신규 서비스 및 시스템의 실용화 이전에 보안 및 안전 기술 개발이 어려움

8

전략 산업의 상용화 시점

보안 영역의 중요성 및 실제 적용 시기에 따른 전략 산업의 상용화 시점은 〈그림 24〉와 같이 이루어질 것으로 예측

〈그림 24〉 전략 산업의 상용화 시점



9

결론 및 정책 제언

■ **결론**

○ 사물인터넷 보안을 포함한 융합 보안 산업 분야는 현재 정부(연 5조 투자)와 민간이 주도하여 공격적인 연구 및 투자 진행 중

○ 재난통신망에 설계초기 단계에서부터 장기간 보안성을 확보하도록 연구

○ 보안 기술의 특성상 시스템(또는 서비스)에 embedded되므로 미래 보안 시장 규모(10~20%)

■ **정책 관련 제언**

○ 국내에서 Best Practice임을 실증 후 신흥국에 시장 개척 전략

○ 중기적으로 ICT 보안 분야 세계 최고의 기술력을 바탕으로 세계 시장 개척

○ 장기적으로 서로 문화가 다른 안전+보안 분야를 win-win 전략을 통해 미개척 분야를 선점할 수 있는 독보적 기술력 보유

- 선순환 구조를 가질 수 있도록 R&D 투자 전략 요구

참고 문헌

[1] 한국정보화진흥원(2015). 국가 재난통신망 기술현황 및 사업추진 방향.

[2] 허정희(2015). 국가 재난통신망 기술현황 및 사업추진 방향. 한국정보화진흥원.

[3] 한국산업마케팅연구소(2013). 2014 정보·물리 보안산업 분야별 시장동향과 유망 기업·기술 현황.

[4] 미래창조과학부(2015). K-ICT 시큐리티 발전 전략.

[5] 한국산업기술평가관리원(2012). 우리나라 산업 기술의 현 주소.

[6] 미래창조과학부(2014). 사물인터넷(IoT) 정보보호 로드맵.

[7] 한국정보통신기술협회(2008). ICT Standardization Roadmap.

[8] ETRI(2009). 로봇 보안 프레임워크 솔루션.

[9] 이준구(2014). 양자암호 네트워킹 연구개발 동향 및 미래. D3-1, KRNET 2014.