KISTEP
2023
22
November

사이버 안보와 디지털 보안 기술의 혁신전략

박지현 연구위원(생명기초사업센터)

Ⅰ. 논의 배경

■ 디지털 기술 의존도가 높아지고 연결성이 강화되면서, 보안 위협, 개인정보 유출 등 정보보안 문제가 개인 사생활 침해뿐만 아니라 국가 안전을 위협하는 요인으로 작용

※ 작년 한 해 전 세계 사이버 공격은 38% 증가, 올해 상반기 국내 사이버 공격은 49%로 지속 증가

■ 러시아-우크라이나 전쟁 사례와 같이 최근 국가 간 전쟁은 물리적 교전과 국가 사회 기능 저하를 위한 사이버 공격이 병행되는 하이브리드전 양상으로 진행

- 정부 기관, 에너지시설, 은행 등 정부·사회 주요 기반 및 방위시설 네트워크 등에 대한 사이버 공격을 통해 적국의 전쟁 수행 능력과 사기를 저하하고 혼란을 야기
- 전쟁 개시 후에는 전 분야 데이터 파괴 공격과 선동 및 군사작전과 연계(방위시설 네트워크)된 사이버 공격 진행

■ 주요 산업 인프라도 에너지, 운송 등 분야별 디지털 전환 확대로 S/W 및 시스템 복잡성이 증가하였으며, AI 도입확산 등에 따른 신기술 위험도 크게 증가

- 과거 주요 인프라의 산업시스템은 폐쇄형 네트워크 중심의 전문 운영기술(OT) 프로토콜과 S/W에 의존했고 인터넷에 연결 없이 이용
- 최근 주요 산업제어시스템(ICS, Industrial Control System)은 인터넷과 연결된 클라우드 이용, 5G 통신망 연결 등 폐쇄형에서 개방형 환경으로 확장

■ 이번 수요포럼에서는 디지털 전환에 따른 사이버 공격의 변화 양상 및 사이버 보안 기술의 발전 패러다임을 살펴보고, 향후 사이버 안보 대응 및 디지털 보안 기술전략 등에 대해 논의하고자 함

제164회 수요포럼 개최 개요
(일시/장소) 2023년 11월 22일(수) 14:00~15:40 / 한국과학기술기획평가원 국제회의실
(토론 좌장) 전승수 KISTEP 사업조정평가본부장
(발　　표) 김정희 한국인터넷진흥원 실장
(패　　널) 윤두식 ㈜지란지교시큐리티 대표이사, 강병훈 KAIST 정보보호대학원 교수

Ⅱ. 현황 및 이슈

■ 사회기반시설, 제조설비 등 다양한 분야의 디지털 의존도가 심화되고 있으며 정보통신, 네트워크 연결 확대로 온·오프라인 경계가 모호해지는 빅블러(Big Blur) 현상이 심화

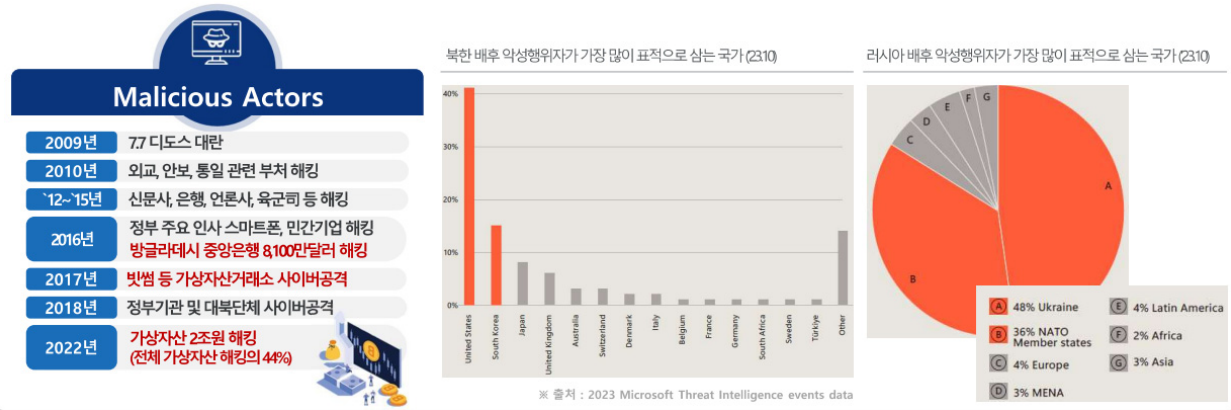
- 디지털화 과정에서 센서들이 연결되고 업무의 안전성 및 생산성이 향상되는 측면이 있는 반면, 보안 측면에서는 제조, 기반 시설의 시스템, SW의 복잡성 증가에 따른 주의가 요구
- 인공지능(AI), 클라우드 등의 혁신기술 도입으로 신기술이 내포하고 있는 위협 요인들에 지속적으로 노출되는 문제를 해결해야 하는 상황
- 최초 영국의 한 병원에서 랜섬웨어가 발생한 이후 지구가 자전하는 방향으로 악성코드가 감염되어 전 세계적으로 파급된 사례

〈그림 1〉 워너크라이 감염 사례

출처 : 제164회 수요포럼 발표자료

■ 악의적인 목적으로 해킹조직을 운영하는 등 국가 배후의 해킹 조직이 정부기관 및 국가 사회기반 시설을 대상으로 위협하거나, 산업기술, 지적재산을 탈취하는 사례가 발생

- 미국의 국가 사이버 보안 전략에 따르면, 사이버 공간의 주요 악성 행위자로 중국, 러시아, 이란, 북한 등을 지명하였으며, 러시아의 경우 세계 1위의 해킹 능력을 보유



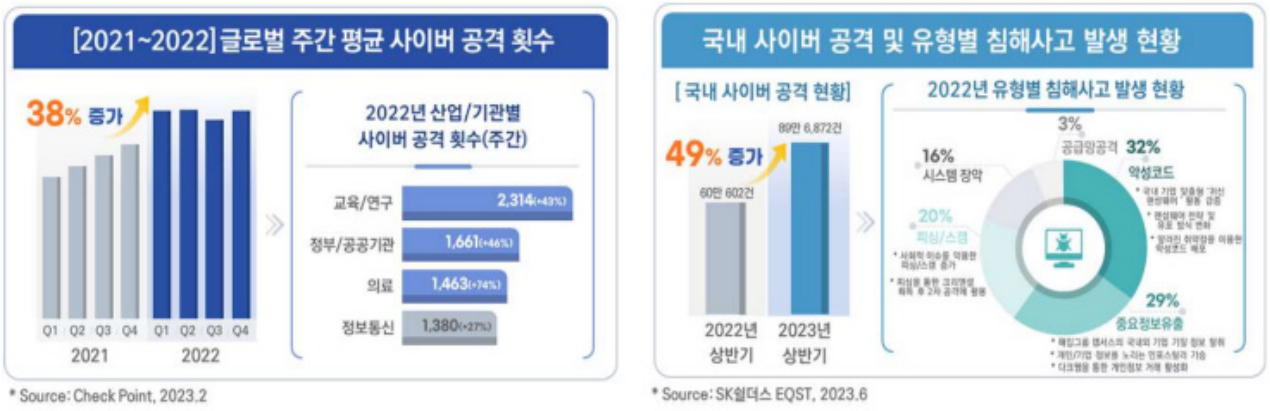
〈그림 2〉 국가 해킹 사례 및 북한, 러시아의 위협 대상국

출처 : 제164회 수요포럼 발표자료

■ 사이버 범죄 관련 서비스를 제공하거나 분업화된 해킹 조직을 운영하는 등 해커 그룹이 기업화되는 경향이 증가

- 사이버 범죄를 정기 구독 방식의 서비스를 제공하는 기업들이 마케팅, 홍보까지 포함하여 대형화된 해커그룹으로 등장하고 있으며, 이들은 가상 자산 등을 탈취
- 글로벌 사이버 공격은 '22년 기준 38%가 증가되어 교육, 정부, 의료 분야로 공격이 확대되고 있으며, 국내 사이버 공격은 '22년 대비 '23년도에 49%가 증가

  ※ '22년 사이버 공격 침해사고 국내 발생 현황: 악성코드 감염 32%, 중요정보 유출 29%, 피싱/스캠이 20% 차지



〈그림 3〉 국내외 사이버 공격 발생 현황

출처 : 제164회 수요포럼 발표자료

■ (러-우크라이나戰) 사회혼란과 마비, 인명피해까지 야기할 수 있는 상황으로 발전하고 있고, 사이버 공격과 물리적 군사 공격이 병행된 하이브리드전 양상으로 발생

- 정부 및 경제 기능 저하를 위해 정부기관 및 사회기반시설을 사이버 공격으로 마비시키고, 데이터 파괴 및 군사작전과 연계한 방위 시설 네트워크 대상 공격 등 군사 작전에 활용

  * 와이퍼(Wiper) 멀웨어, 디도스(DDos) 등 사이버 공격 수법 사용

- 동맹국 및 국제기구(NATO)는 사이버 공격에 맞서 우크라이나를 지원하고, 민간의 빅테크 기업들은 혁신기술을 활용해 파괴적 공격의 사전 징후를 감지하고, 방어 코드를 신속하게 보급하는 역할을 수행

〈그림 4〉 러-우크라이나 사이버 공격 현황 및 공격 수법

출처 : 세계일보, 제164회 수요포럼 발표자료

■ (사회기반/제조설비 공격) 기존의 제조산업이 비즈니스 시스템과 통합되고 개방형 환경으로 변화됨에 따라 사이버 공격 위협이 증가되고, 경제적·사회적 막대한 피해로 연결

- 에너지 분야가 상당 부분 디지털화 되면서, 미국 콜로니얼 파이프라인社 랜섬웨어 감염 시 송유 서비스가 중단되고, 국가 비상사태가 선포될 정도로 피해가 심각

  ※ 미국 동부 해안 지역 8.900km 연료 공급 중단 및 연료 가격이 최고가('14년 이후 $2.98/Gal)를 갱신

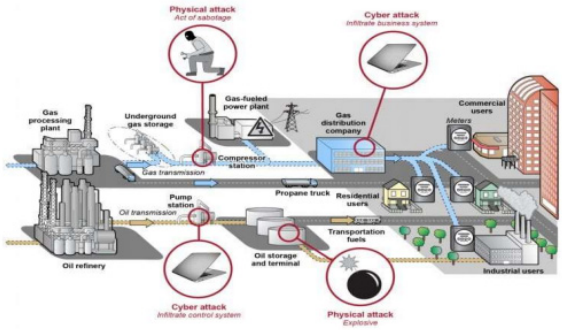
- 세계 4위의 알루미늄 제조사인 노르스크 하이드로社는 랜섬웨어 공격을 받아 제련소, 용광로, 자동화 공정 일부를 수개월 동안 중단함으로써 막대한 경제적 손실 발생

  ※ 전 세계 알루미늄 가격 1.2% 급등 및 공정 중단으로 약 $8,400만(약 1,141억 원) 규모의 피해

현대의 에너지 산업 분야는 상당 부분 **디지털화**,
필요한 장치들의 대부분이 **컴퓨터를 통해 제어되는 형태**로 운영

송유관의 디젤과 휘발유 연료의 흐름을 관리하고 제어하기 위해
압력 센서, 온도조절 장치, 밸브, 펌프 등이 사용

이러한 운영기술(Operational Technology)들이 중앙 시스템으로 연결된 구조

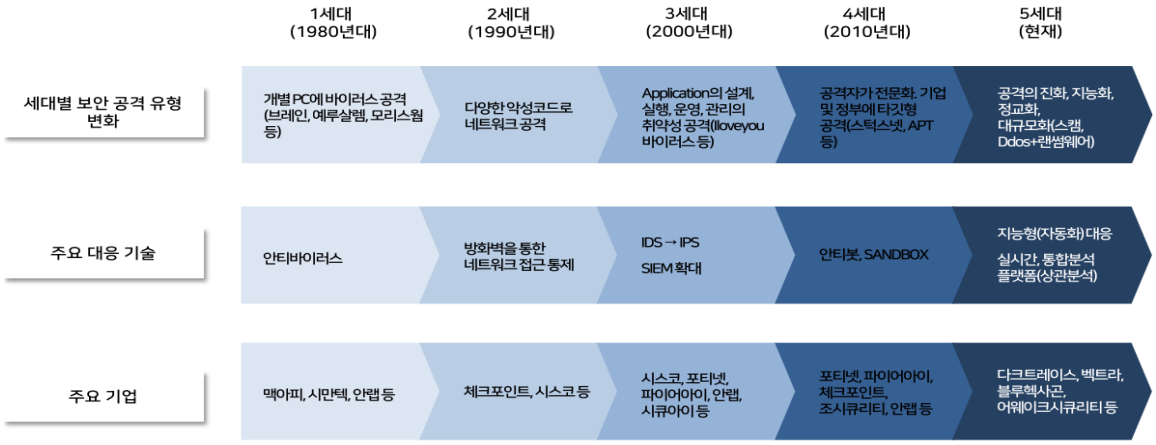


〈그림 5〉 미국 송유관 기업(콜로니얼 파이프라인)의 랜섬웨어 감염 사례

출처 : U.S. Government Accountability Office, 제164회 수요포럼 발표자료

■ 사이버 공격은 세대별 발전을 거듭하여 국가 안보 차원으로 인식되고 있으며, 사이버 공간 악성 행위 근절을 위한 국가 차원의 책임성과 국가 배후 해킹 집단 근절 노력이 강조

- 보안 위협은 3세대 이후 사이버 공격이 본격화되었으며, 4세대를 거쳐 5세대에 이르러 인공지능(AI) 도입 등 새로운 유형의 사이버 공격과 정보보안 역량이 향상되는 방향으로 진화



〈그림 6〉 세대별 사이버 보안 공격의 발전 흐름

출처 : 한국인터넷진흥원(2021)

- 5G 통신장비, 반도체, 인공지능(AI) 등에 대한 미·중 기술패권 경쟁의 일환으로 미국은 데이터 갈취 등 국가 안보 위협이 되는 장비 도입을 제한하거나 반도체 중국 수출을 전면 금지

- 대규모 해킹을 통해 취득한 가상자산을 핵무기 개발 자금으로 조달하는 등 해킹으로 인한 수익을 국가안보 대립의 재원으로 활용하는 정황들이 국제사회에 보고

■ 비대면, 클라우드 등 변화된 환경을 악용한 사이버 공격이 증가하고 있어 사고 사례 분석을 통한 보안 요소별 대응 전략 필요

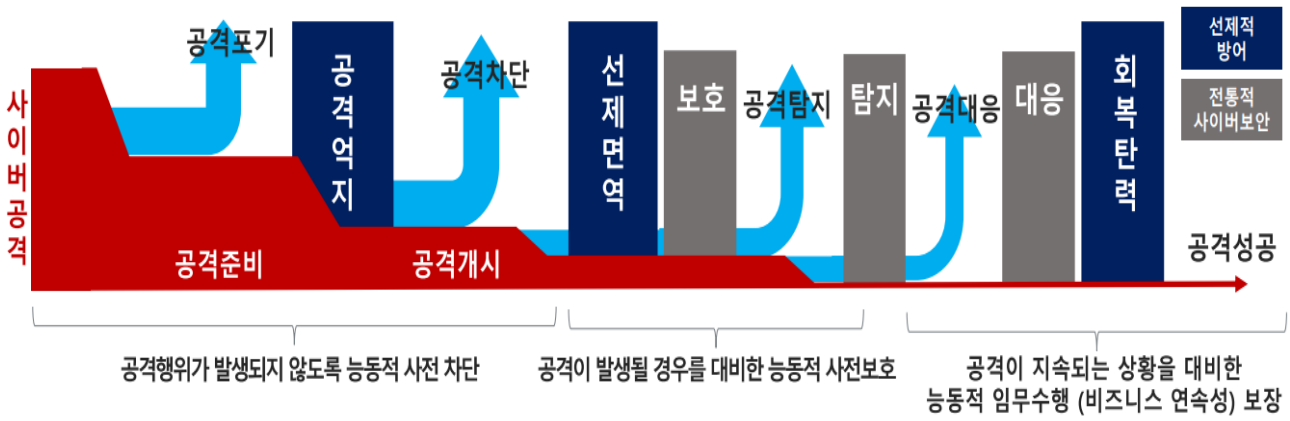
- 정보 유출, 랜섬웨어, 웹변조, 디도스 등이 지금까지도 계속 발생되고 있으며, 민간 사고 발생 시 네트워크 및 데이터 침해 등 가장 취약한 부분에서 문제가 발생
- 기존의 보안 접근이 조직 내에서 정보 자산 보호를 위한 경계 기반의 보호 체계라면, 변화된 환경에서는 경계 기반 뿐만 아니라 내부 데이터 보호를 위한 상시 검증 전략을 동시에 구현시킬 필요

〈그림 7〉 변화된 환경을 악용한 공격 유형

출처 : 제164회 수요포럼 발표자료

■ 사이버 공격에 대한 탐지·대응에서 선제적, 능동적 방어 전략의 일환으로 억제(Deterence) 중심으로 기술 개발하여 혁신기술을 통한 변화를 유인

- 사이버 보안 기술을 개발 함에 있어 악의적 행위자들의 잠재적 사이버 공격을 사전에 식별하고, 사이버 공격 경로를 사전에 예측하여 활동 초기에 차단
- 사고가 발생하더라도 정상적인 서비스로 빠르게 돌아갈 수 있는 복원력을 확보하는 역량과 공격 이후 복구, 적응 등 메커니즘을 확보할 수 있는 관련 기술개발에 집중



〈그림 8〉 사이버 공격에 대한 억제 중심의 기술개발 전략

출처 : 제164회 수요포럼 발표자료

Ⅲ. 시사점

■ 사이버 공격에 선제적으로 대응할 수 있도록 인공지능(AI), 클라우드 등 신기술 기반의 보안 기술 경쟁력 확보 및 고도화

- 구글, MS 등은 파트너쉽 기반의 통합형 보안 플랫폼에 적용하여 보안 시장에서의 주도권을 확보하려 하고 있으나, 국내는 네트워크 환경에서의 사이버 위협에 대한 대응 역량이 부족
- 신기술 활용을 통한 효과적인 보안관리 체계 강화 및 보안 기술 자체를 고도화, 효율화하는 방향으로 핵심기술 확보 필요
- IoT 등 초연결에 초점을 두고 기술이 발전되었으나, 사이버 네트워크 등 안전한 사이버 공간을 확보할 수 있는 기술개발을 우선할 필요

■ 국가 안보와 국민 안전을 위해 정교화된 사이버 공격에 대비한 사회간접자본(SOC) 대상 보안 내재화 및 국가 간 공조 차원에서의 글로벌 협력 확대

- 국내 기술력으로는 전력 등 일부 분야에서 상당 부분 보안 기술이 내재화되어 있으나, SOC 분야는 시스템 내에서의 보안 기술 내재화가 시급
- 국가 간 사이버 범죄 수사 등 협력에 적극적으로 대응하고, 사이버 공격 등 글로벌 공격에 대비한 선제적 안보 역량 및 글로벌 협력 기능 강화

■ 네거티브 규제 도입 등 보안 시장 확대를 위한 기반 조성 및 기업 수요 등을 고려한 국내 산업 경쟁력 확보

- 보안 수요 기업들이 서비스, 솔루션 도입 시 장비를 자사에서 놓고 구현해야 하는 상황에서 클라우드 등의 환경변화에 대응하기 위한 서비스 및 관련 역량이 글로벌 대비 취약한 편
- 국내 산업은 통합형이라기 보다 부분적으로 특화되어 있고, 미국, 일본 대비 시장 규모가 작기 때문에 기술개발 뿐만 아니라 시장 성장도 우선 고려할 필요
- 산업별 제품 서비스 개발을 위한 전 라이프사이클에서의 보안을 보장할 수 있도록 경계 안·밖의 보호 대상 다양화로 보안 접근방식 제고

■ 서비스화된 사이버 공격에 대한 보안 역량을 강화하기 위해서는 정부와 민간과의 협력 확대 및 정부의 마중물 역할 강조

- 민간의 사이버 위협정보 분석·공유 시스템(C-TAS*), 상시 훈련을 지원하는 사이버보안 훈련 플랫폼 등 민관 협력차원에서 기술개발에 활용 될 수 있도록 다양한 재원을 정부, 민간이 공유하고 기술 고도화에 활용될 수 있도록 협력

  * Cyber Threat Analysis & Sharing : 사이버 공격 및 산업 정보침해 사고에 대응하기 위해 한국인터넷진흥원에서 운영하고 있는 시스템으로 보안기업, 금융, 전자상거래 등 다양한 분야의 기업이 참여하여 위협정보를 공유

- 정부가 제시한 사이버 보안 시장 30조 원 목표(2027년까지)를 달성할 수 있도록 관련 예산 확보 노력과 범정부 차원의 예산 소요 계획 등 마련 필요