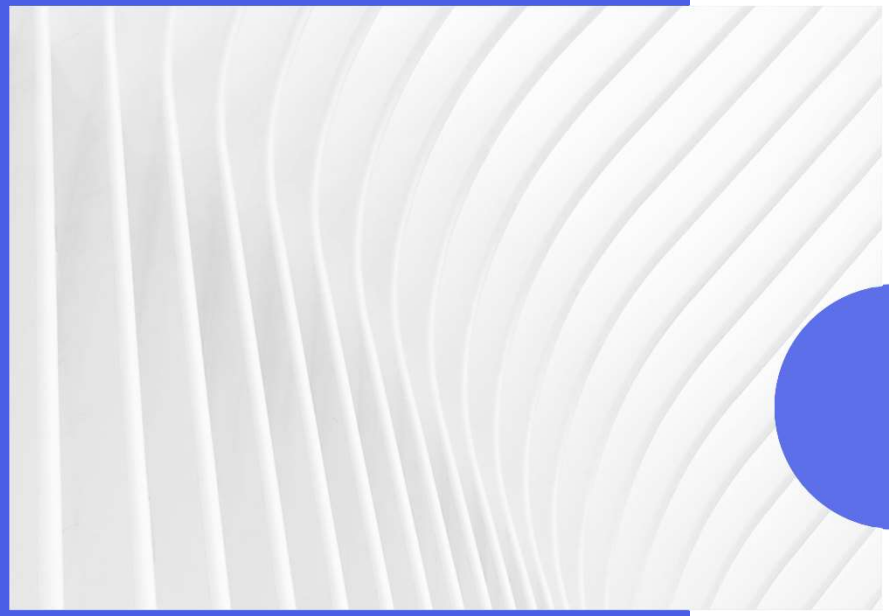
사이버안보와 디지털 보안 기술의 혁신 전략

한국인터넷진흥원
(Korea Internet & Security Agency)
김정희 실장

AGENDA



01 논의 배경

02 현황 및 주요사례

03 정책 대안

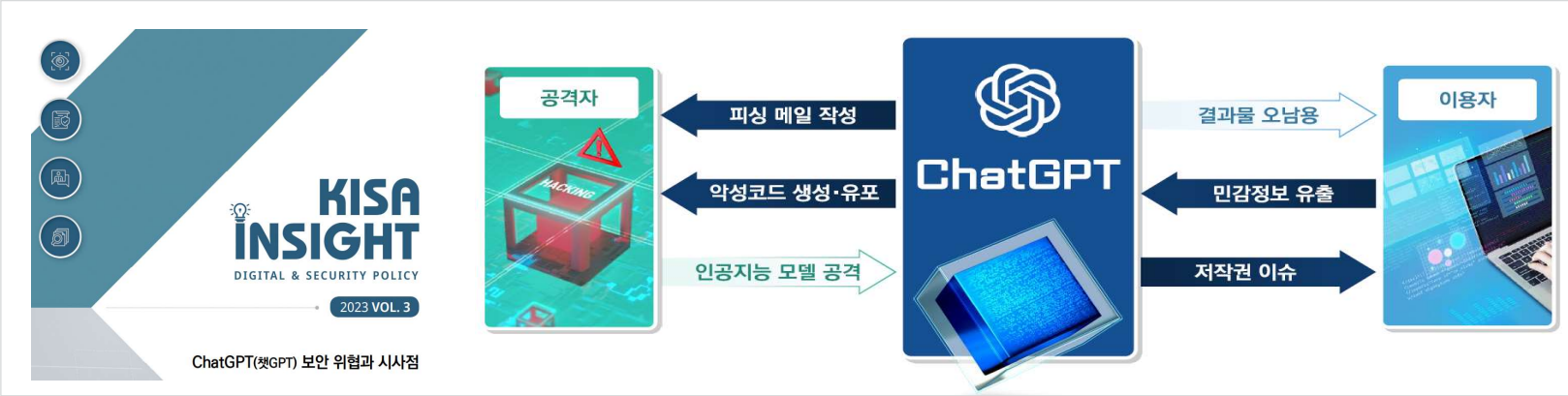
논의 배경

디지털 의존도 심화

정보통신·NW 연결 확대로 온·오프라인 경계 모호, "빅 블러(Big Blur)" 현상

- **전력, 가스 등 사회기반시설과 제조 분야의 디지털화 → 이를 구성하는 SW 및 시스템 복잡성 증가**
  - (사회기반시설) 인공지능(AI)과 로봇의 결합, 디지털 트윈 도입을 통해 업무 안전성 증대
  - (제조) 현장 데이터 통합, 무선네트워크 및 센서 등 인프라를 전 공정과 연계하여 생산성 및 효율성 향상

- **인공지능(AI), 클라우드 등 도입 확산 → 신기술 관련 위협 지속**
  - ChatGPT – 피싱 메일·스팸, 멀웨어·랜섬웨어 생성, 취약점 노출, 민감데이터·개인정보 노출, AI에 대한 공격 등

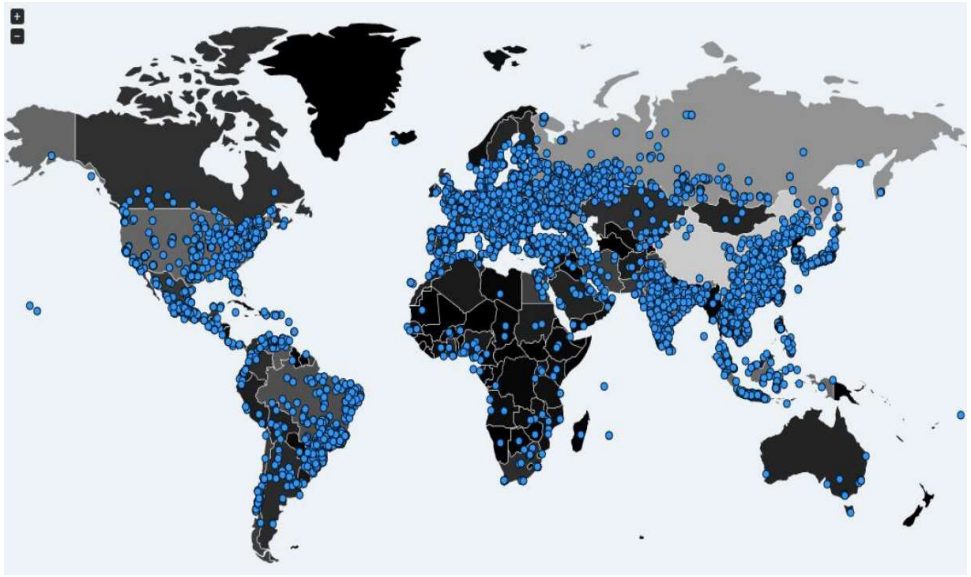


디지털 의존도 심화

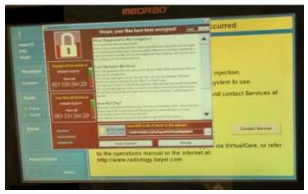
정보통신·NW 연결 확대로 온·오프라인 경계 모호, "빅 블러(Big Blur)" 현상

- 글로벌로 연결된 인터넷 상호연결성 → 사고에 따른 영향이 전 세계로 실시간 확산
  - 글로벌로 확산되는 사이버공격의 위험성을 일깨워준 대표적 사례 : 워너크라이 공격

<워너크라이 감염 지도>



병원 서비스 마비

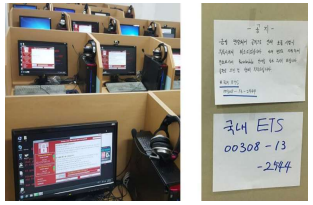


공항 서비스 마비

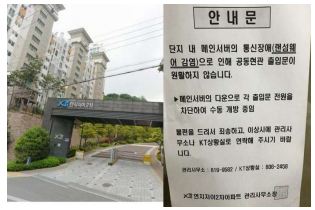
철도 서비스 중단

영화 상영 중단

토플 시험 중단



아파트 출입 정지



악의적 행위자들의 사이버 능력 강화

국가 배후 해킹 조직으로 활동하는 악성 행위자의 공격

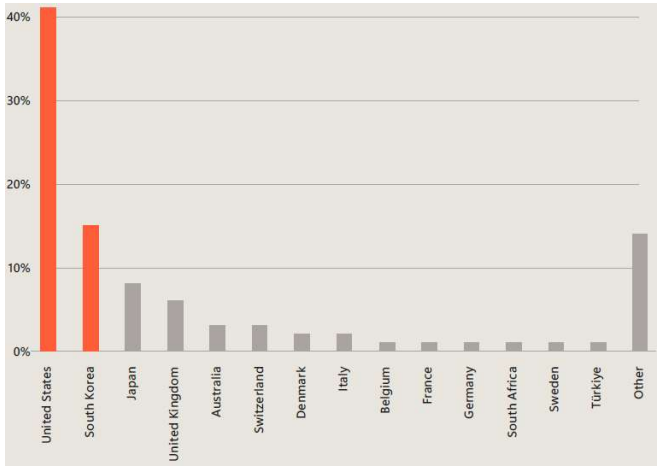
정부기관 및 국가 사회기반시설 대상 위협, 산업기술·지적재산 탈취

- (美) 국가 Cybersecurity 전략에서 사이버공간의 악성행위자로 China, Russia, Iran, North Korea를 지명

Malicious Actors

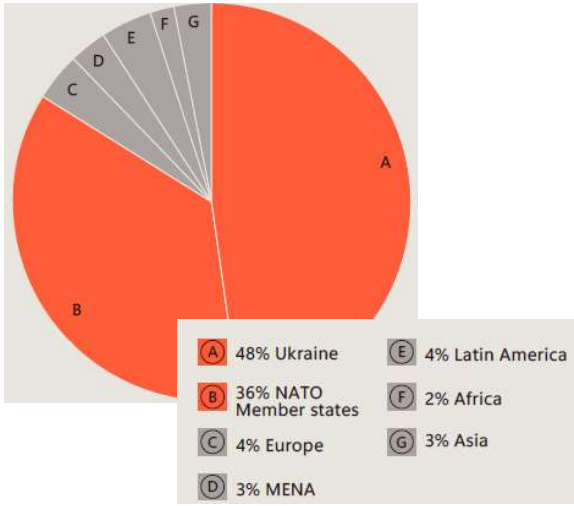
2009년	7.7 디도스 대란
2010년	외교, 안보, 통일 관련 부처 해킹
`12~`15년	신문사, 은행, 언론사, 육군회 등 해킹
2016년	정부 주요 인사 스마트폰, 민간기업 해킹 방글라데시 중앙은행 8,100만달러 해킹
2017년	빗썸 등 가상자산거래소 사이버공격
2018년	정부기관 및 대북단체 사이버공격
2022년	가상자산 2조원 해킹 (전체 가상자산 해킹의 44%)

북한 배후 악성행위자가 가장 많이 표적으로 삼는 국가 (23.10)



※ 출처 : 2023 Microsoft Threat Intelligence events data

러시아 배후 악성행위자가 가장 많이 표적으로 삼는 국가 (23.10)



악의적 행위자들의 사이버 능력 강화

해킹 비즈니스는 가파르게 성장, **고성장을 멈추지 않는 산업**

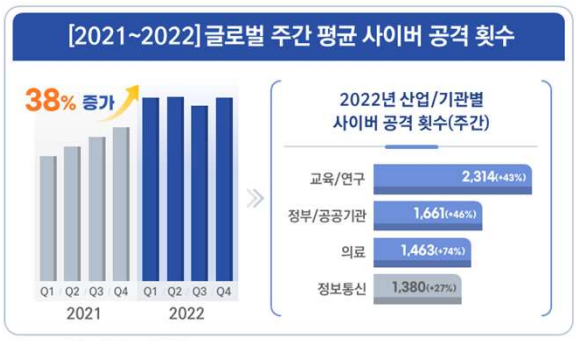
사이버범죄를 서비스로 제공하는 기업 등장, Crime as a Service(CaaS, 사이버범죄의 서비스화)

- 정기 구독방식의 범죄서비스 제공

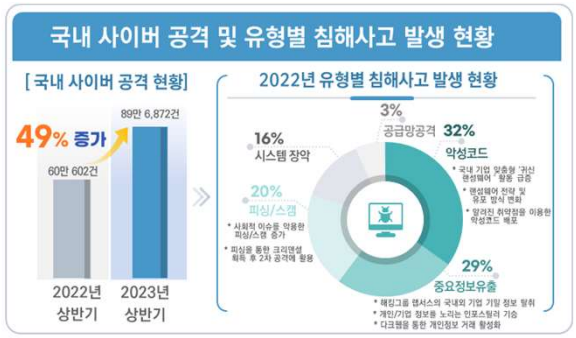
서비스형 랜섬웨어를 악용한 대형 해커그룹 (멀웨어 개발, IT인프라, 마케팅, 홍보,고객지원 등 분업화된 조직 구성) → **가상자산 탈취**

다크웹 사이트 등에 **평균 4시간 마다 1개 조직의 피해** 게시('22년 피해 조직 : 2,679개, 전년대비 **4% 증가**, 피해자 **41%가 협상**)
(원인) ① 서비스형 랜섬웨어 부상, ② 높은 랜섬웨어 수익률 ③ 개인정보 유출 등에 따른 과태료

'22년 글로벌 사이버 공격 38% 증가, 교육·정부·의료 분야 공격 확대



* Source: Check Point, 2023.2



* Source: SK쉴더스 EQST, 2023.6

- '23년 상반기 국내 사이버 공격 49% 급증

악성코드 감염이 32%로 가장 높았으며,
중요정보 유출 29%, 피싱/스캠이 20% 차지

국가안보 차원의 문제로 인식

✔ 사이버공격은 국민생명·안전을 위협하는 수준을 넘어 국가 안보 문제로 접근

> Cybersecurity는 미국 경제의 기본 기능을 수행하고, 주요 인프라를 운영하며, 민주주의와 민주주의 제도를 강화하고, 데이터 및 통신상의 개인정보를 보호하고, 국가를 방위하는데 있어 필수 기능
>
> ※ 출처 : 미국 국가 Cybersecurity 전략

✔ 5G 통신장비, 반도체, 인공지능(AI) 등에 대한 미·중 기술패권 경쟁 심화

- 데이터갈취 등 백도어 이슈로 국가 안보에 위협이 되는 장비 도입 제한 ('22.11, 美 보안장비법 개정)
  - 화웨이, ZTE, 하이테라 커뮤니케이션, 하이크비전 테크놀로지, 다후어 테크놀로지 등
- 美, AI 개발이 군사력으로 이어져 국가안보 위협 → 관련 반도체 중국 수출을 전면 금지 ('22.10)
  - 대통령 행정명령(EO) 'Safe, Secure, and Trustworthy AI' ('23.10, 백악관)

✔ 해킹을 통해 취득한 가상자산 → 핵무기 개발 자금으로 조달 정황 제기

- 대규모 해킹을 통해 발생된 수익을 현실의 국가안보 대립의 재원으로 활용

국가안보 차원의 문제로 인식

✔ 사이버공간 악성행위 근절을 위한 **국가 차원의 책임 있는 행동**과 **국가 배후 해킹 집단 근절** 노력 강조

한·미 전략적 사이버안보 협력 프레임워크('23.4월)

사이버공간의 악의적 행위자에 대한 능동대응 강조

※ 출처 : 국가안보전략

Five Eyes 정보동맹국 및 유사입장국

사이버공격 정보공유 및 악의적 행위자 공동제재,
사이버외교, 글로벌 규칙 제정 움직임(사이버범죄조약, 탈린매뉴얼)

※ 그림출처 : 매일경제(2021.07.19)

현황 및 주요 사례

사이버위협으로 인한 피해 양상

금전적 피해

개인·기업의 금전적 피해

기업 피해 정육업체 JBS SA 랜섬웨어 피해

송유관 이어 최대 정육업체 해킹 … 美 "러시아 범죄 조직 소행"

중앙일보 | 2021. 06. 02

개인 피해 스마트홈 월패드 해킹으로 사생활 유출

내 집서 알몸으로 다녔는데… 실시간으로 찍혀 팔리고 있었다

중앙일보 | 2021. 11. 26

사회적 혼란

국가 간 사이버공격으로 인한

사회 혼란과 마비

국가 안보 초연결시대, 사이버전쟁 발발

우크라이나에 디도스 공격 … 정부·은행 사이트 마비

중앙일보 | 2022. 02. 24

사회 불안 해킹된 웹사이트 접속불가 사태

신원 미상 해킹그룹, 우리말학회 등 12곳 해킹

중앙일보 | 2023. 01. 26

실생활 위협

국민 생활 위협 및 인명 피해 발생

사회전반 피해 사회기반 시설에 대한 공격

미국 방사성폐기물보관소 해킹… 러시아 해커 조직 수행 추정

한국일보 | 2023. 06. 16

일상 마비 주요 통신사 해킹

LG유플, 고객DB 암호 관리 부실로 원격 해킹에 약 30만명 정보 유출

경향신문 | 2023. 4. 27

디지털 전환으로

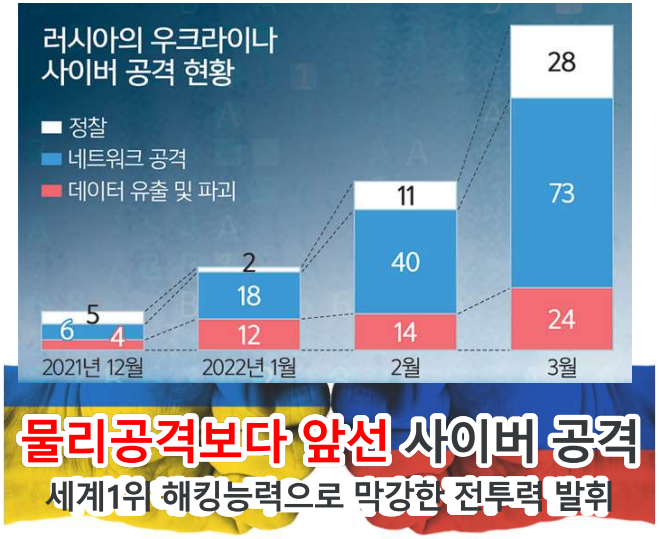
사이버보안의 범위 및 기능·역할 변화

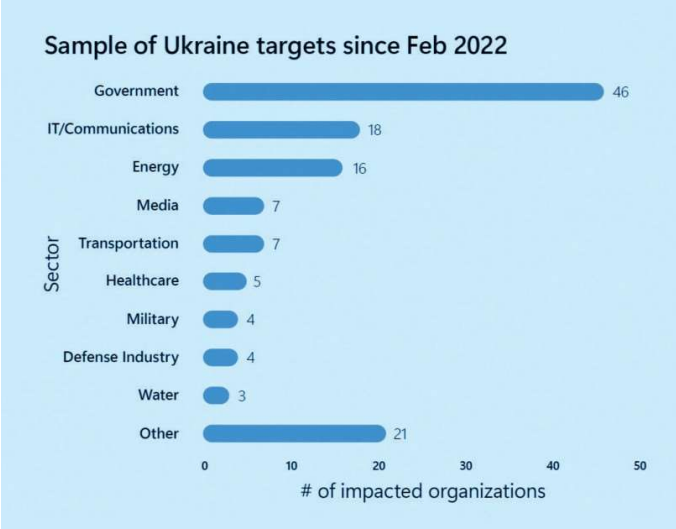
국민 생명을 넘어 국가 안보까지 고려

러-우크라이나戰의 사이버 공격

러시아의 침공은 **사이버 공격**과 물리적 **군사 공격**이 병행된 **하이브리드戰** (‘22.2)

- **정부기관 및 사회기반시설**을 사이버 공격 → 러시아의 **군사 작전에 용이한 환경** 조성
  - (침공 전) 정부 및 경제 기능 저하(정부기관, 에너지시설, 은행 대상), 정보 통제·조작(미디어시설, 인터넷공급자 대상)
  - (침공 후) 전 분야 데이터 파괴 공격, 군사작전과 연계된 공격(방위 시설 네트워크 대상)





< 우크라이나戰 사이버 공격 수법 >

와이퍼(Wiper) 멀웨어

- 우크라이나 內 특정 영역에만 유포되도록 설계
- 먼저 수백대의 컴퓨터를 손상시킨 후, 수 천대 다른 컴퓨터의 데이터 및 SW 파괴

디도스(DDos)

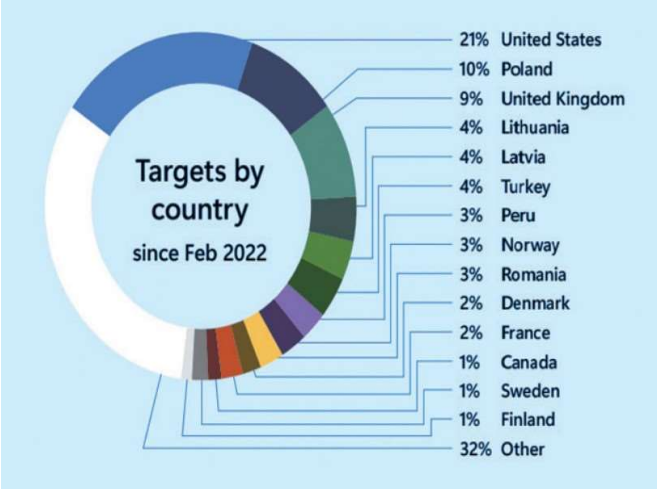
- 서버와 네트워크가 감당할 수 없는 트래픽을 순간적으로 일으켜 서비스를 마비 시키는 기법

시사점 (사이버戰)

» 우크라이나 동맹국에 대한 사이버 공격 동시 진행

- 동맹국 및 국제기구(NATO)는 사이버공격에 맞서 우크라이나 지원
  - (미국) 러시아 침공 이전부터 사이버사령부, 민간 전문가를 파견하여 안보전략 수립 및 역량강화 지원
  - (북대서양조약기구) 공격 방어를 위한 사이버 신속대응팀 파견

- 러시아는 42개국 128개 기관 대상 정보통신망 침투활동 및 공격



- 러시아는 주변국과 분쟁 시 마다 대규모 사이버 공격 감행
  ('07년 에스토니아, '08년 조지아, '14 크림반도 등)

☑ 다양한 형태의 공격을 미리 감지하고, 방지할 수 있는 역량

☑ 동시다발적으로 발생하는 공격 대비 대규모 실전 대응 훈련 역량

시사점 (사이버戰)

» 민간의 빅테크 기업이 공개적으로 전장에 직·간접 참여하여 지원

- 최근 발전된 사이버위협 인텔리전스 및 엔드포인트 보안 기술 활용
  - 사전에 AI 사용을 포함한 위협인텔리전스 기술로 우크라이나 정부기관 및 기업(4곳) 대상의 파괴적 공격 징후를 효과적으로 감지
  - 엔트포인트 보안을 통해 클라우드 서비스 및 기타 연결된 장치에 방어코드를 신속하게 배포, 악성행위 식별 및 비활성화

☑ 공격 그룹이 자행하는 위협 식별, 사전에 위협을 방지할 수 있는 대응 체계

» 국경 너머 타 국가로 데이터 자산을 분배·분산하고, 운영을 지속

- 타 지역에서 관리되는 클라우드로 디지털 인프라를 신속하게 분산, 민간과 군사작전 성공적 유지

☑ 블랙아웃(대정전, 통신마비 등) 상황에서도 사회기반시설이 정상 운영 할 수 있는 체계

사회 기반시설 사이버 공격 (콜로니얼 파이프라인)

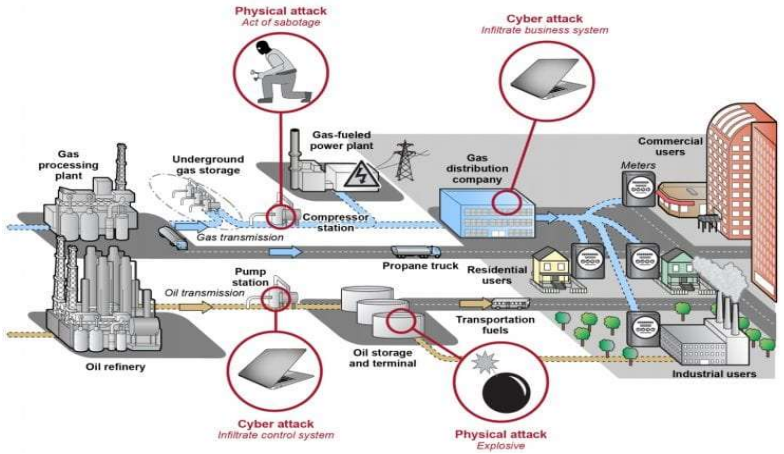
美 최대 송유관 기업의 **랜섬웨어 감염**으로 **송유 서비스 중단**, **국가비상사태** 선포('21.5)

- **랜섬웨어 감염으로 데이터가 유출, 동부 해안 지역 8,900km 연료 제공 중단**
  - 콜로니얼 파이프라인의 요금 청구 시스템 해킹을 통해 데이터를 암호화, 해당 몸값($440만, 약 60억원) 요구
  - 행정부는 텍사스, 뉴욕 등 동·남부 17개 주, 워싱턴 DC 등 18개 행정구역 국가 비상사태 선언
  - (FBI) 랜섬웨어 공격자 가상자산 지갑에서 230만 달러 압수
- **해당 사고로 기름 사재기 등 연료 가격 '14년 이후 최고가 경신(2.98달러/Gal)**

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



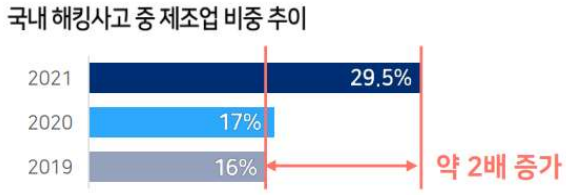
제조 설비 사이버 공격 (노르스크 하이드로)

세계 4위 알루미늄 제조사의 **공장 제련소, 용광로, 자동화 공정** 일부 **수개월간 중단** ('19)

- **랜섬웨어 공격으로 노르웨이 본사를 비롯해 미국, 브라질, 카타르 등 공장 생산 중단**
  - Norsk Hydro는 알루미늄 제품 생산에 필요한 모든 공정을 포함하는 제조 공장과 더불어 원자재 채굴, 수력 발전소을 함께 운영하는 세계 4위 제조사
  - 사고 직후 공정을 수동으로 전환하는 등의 조치를 취했으나 일부 공장의 경우 수개월간 폐쇄
- **전 세계 알루미늄 가격 1.2% 급등, 공정 중단으로 약 $8,400만(약 1,141억원) 경제적 손실**

1위 2020년 글로벌 시장에서 **제조산업의 해킹 피해 비중 순위**(24.4%)

29.5% 2021년 상반기 국내 해킹 사고 중 **제조산업이 차지하는 비율**



시사점 (사회기반시설·제조설비 사이버공격)

» 폐쇄형 환경으로 안전하다는 잘못된 인식

- 과거 외부 네트워크와 분리해 내부 장비들만 생산 순서대로 연결하는 독립된 폐쇄형 환경으로 구축
- (서비스 중지에 대한 반감) 패치 업데이트 및 리부팅에 대한 부담
- USB를 통한 악성코드 감염, 산업 제어 설비 유지보수 시 외부 연결

» 산업 설비 제조사 마다 서로 다른 전용 프로토콜과 OS 사용

- (제조사 중심의 개발규격) 가용성을 중시하는 특성으로 보안 솔루션 적용에 회의적, 배타적
- 설비 및 네트워크 안전성에 대한 모니터링과 관리에 애로, 실시간 감지와 제어가 어려움
- 산업 설비 보호를 위한 자산 식별과 복잡한 시스템에 대한 가시성 확보에 어려움

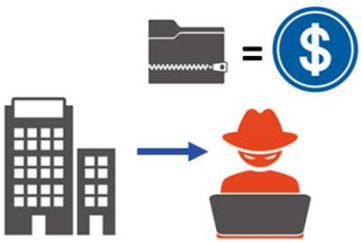
» IoT, Cloud, 5G 확대로 연결되는 기기 서비스 증가

- 기존 비즈니스(IT) 시스템과 통합되고 개방형 환경이 점차 증가
- Edge 보안의 증가

변화된 환경을 악용한 공격

✔ 랜섬웨어 감염, 개발 소스코드 및 내부 사용자 계정 탈취, 개인정보 유출, 웹변조, 디도스 등 지속

☑ 기존 경계기반 뿐 아니라 내부 데이터 보호를 위한 “Never Trust, Always Verify“ 전략



- **정보유출**

유명 기업의 중요 자료를

유출 후 SNS에 공개

⇒ **금전 협박 & 능력 과시**

- **랜섬웨어**

중앙 관리 서버 및 백업

서버를 최우선 공격

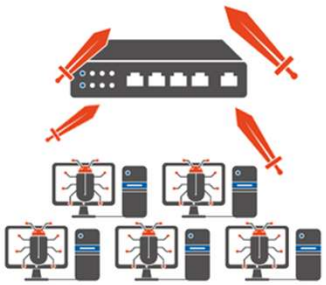
⇒ **피해 파급력 극대화**

- **웹변조**

영세하지만 고정 방문자가

있는 사이트를 변조

⇒ **충격 극대화**



- **디도스**

주요 네트워크 장비 대상 공격

⇒ **불특정 다수 피해자 유발**

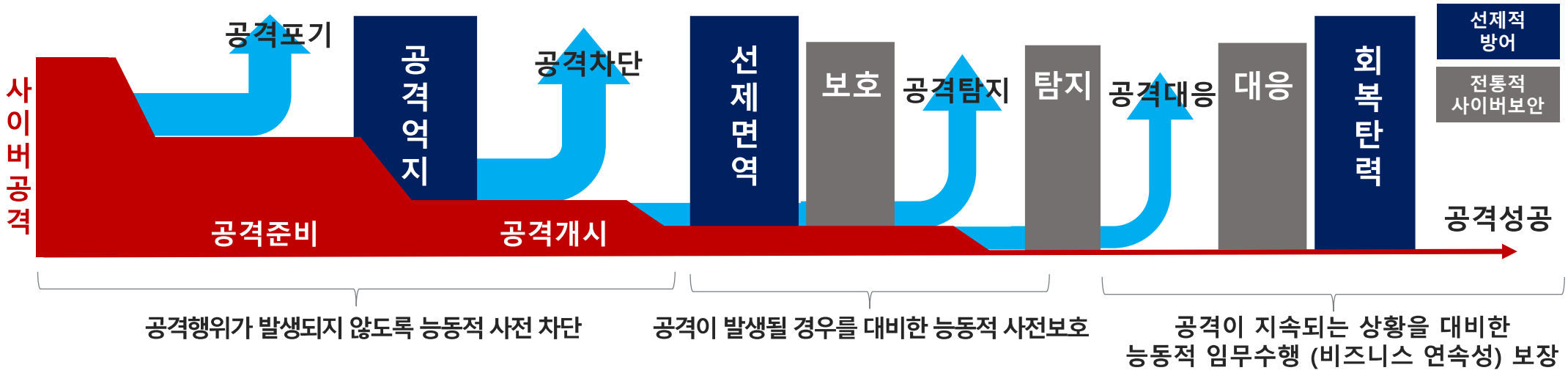
정책대안

사이버 억제 중심의 접근

☑ 사이버공격에 대한 탐지·대응에서 억제(Deterrence) 중심의 기술개발

사이버공격에 소요되는 비용을 증가시켜 공격자가 얻는 이익을 줄임으로써, 공격의지 약화 유도 전략
(구체적 방법론) 선제적, 능동적 방어 | (억제) **공세적 사이버역량, 능동적 사이버방어**

악의적 행위자들의 움직임을 사전에 관찰, 추적하여 활동 초기 단계에 선제적으로 방해하거나 중지시킬 수 있는 역량
사고가 발생 하더라도 정상적인 서비스로 빠르게 돌아갈 수 있는 복원력 강화



혁신기술을 통한 변화 유인

☑ SoC, 자동차·반도체 제조·생산시설의 디지털化

- **인터넷/5G 연결이 확대되는 SoC(사회 기능 유지를 위해 운영되는 필수 시설·설비) 대상 보안내재화**
  - 전력, 도시가스, 수도, 도로/철도/ 공항/항만, 댐 상하수도 시설, 통신시설, 방송 등 국방, 의료, 금융
  - 보안은 IT영역에서 OT 영역으로 확대 적용
  - ICS를 위한 Asset Detection, 시스템에 장애가 발생해도 서비스를 유지할 수 있는 결함감내(fault tolerance) CPS, ICS 패치 자동화, ML 적용된 SCADA IDS 이상감지, SIEM에 물리적 센서 통합관리

☑ 인공지능(AI), 클라우드 등 新기술 기반의 기술 고도화 및 효율화

- **구글, MS, IBM 등은 M&A 및 파트너십 기반으로 통합된 보안 플랫폼 구축을 통해 보안시장의 주도권을 확보하려는 전략 구사**
  - 단품 솔루션에서 통합 보안 플랫폼으로의 변화, 클라우드 보안/AI 보안 기술들 적용
  - 공동 · 협업 통합보안 사업화 모델, 표준화 및 상호운용성 확보 필요
  - 통합보안 모델(예시): 이벤트 로그(SIEM) + 엔드포인트 보안(EDR) + 자동화된 통합관제(SOAR)가 결합 등
- **양자내성암호, 프라이버시강화기술(PET)**

국가안보, 국민안전을 위한 사이버 대응력

☑ 정교화된 사이버공격 대비한 全 산업 보안관리체계 확립

- 산업별 제품서비스 개발을 위한 전 라이프라이클에서 보안 보장
  - Security by default/design, 취약점 handling | SBOM(S/W Bill of Material) | ZTA(Zero Trust Architecture) 등 | 경계 안·밖의 보호대상 다양화로 보안 접근방식 제고
  - 선제적으로 보안을 고려할 수 있도록 조달, R&D 과정의 요구사항 강화

☑ 서비스화 된 공격에 대비한 정부차원의 마중물 제시와 민관협력

- 사이버 위협정보 분석·공유 시스템 활용
- 민간 분야 상시 훈련 – 사이버시큐리티 훈련 플랫폼

감사합니다

Korea Internet & Security Agency(KISA)

www.kisa.or.kr / www.boho.or.kr