

# 대한민국 사이버안보 확립 방안

고려대학교 정보보호대학원

석좌교수 임종인

1. 사이버보안 주요 이슈와 현황
2. 사이버보안 패러다임의 변화
3. 대한민국 사이버안보 확립 방안
4. 결론 및 시사점

## 1. 사이버보안 주요 이슈와 현황

# 사이버보안 주요 이슈와 현황

## ◆ 한-미 정상회담과 사이버안보 협력

- 2023년 4월, 미국에서 열린 한-미 정상회담에서 양국 동맹의 범위가 사이버공간으로 확장을 합의하는 등 협력을 강화했으며 이를 포괄하는 '전략적 사이버안보 협력 프레임워크' 채택



APRIL 26, 2023

### Leaders' Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea

President Yoon and President Biden recognized that the Alliance applies to cyberspace and committed to establish a U.S.-ROK Strategic Cybersecurity Cooperation Framework. The United States and the ROK commit to using this framework to expand cooperation on deterring cyber adversaries, increase the cybersecurity of critical infrastructure, combat cybercrime, and secure cryptocurrency and blockchain applications. The Presidents expressed concern regarding the DPRK's illicit cyber activities that fund its unlawful WMD and ballistic missile programs and committed to expanding information sharing and enhancing international awareness to combat DPRK cyber threats and block its cyber-enabled revenue generation.



다시 대한민국!  
새로운 국민의 나라

※ 엠바고 : 한미정상회담 발표 후 보도 가능 (별도 공지) 배포 : 2023년 4월 일( )

### 한미 정상, 전략적 사이버안보 협력 문서 채택

- 시대의 흐름속에 진화하는 사이버안보 동맹 -

윤석열 대통령은 4.26. 워싱턴에서 바이든 미국 대통령과 정상회담을 갖고 양국간 주요 안보·경제 현안에 대해 협의하였습니다.

양 정상은 한미동맹 70주년을 계기로 진화하는 시대의 흐름에 맞춰 그간의 한미동맹을 사이버 공간까지 확장하기로 선언하였으며, 그에 따라 “전략적 사이버안보 협력 프레임워크”(이하 협력 문서)를 공동으로 발표하였습니다.

\* Strategic Cybersecurity Cooperation Framework

### STRATEGIC CYBERSECURITY COOPERATION FRAMEWORK BETWEEN THE REPUBLIC OF KOREA AND THE UNITED STATES OF AMERICA

In commemoration of the 70<sup>th</sup> anniversary of the United States (U.S.) and the Republic of Korea (ROK) Alliance, we intend to make robust and resilient national cybersecurity a high policy and strategic priority, including responding to the upsurge in national security threats while contributing to peace and prosperity in cyberspace.

# 사이버보안 주요 이슈와 현황

## ◆ 주요 이슈 (1) ChatGPT와 A.I.

- ChatGPT로 촉발된 A.I.의 발전은 사이버보안에도 많은 파급 효과를 미칠 것으로 예상되며 A.I. 활용 공격에 대한 대응이 필요하며 보안에 A.I. 활용하는 서비스들도 예상되고 있음

INSIDER

HOME > TECH

### UK spy agency says AI chatbots like ChatGPT pose a security threat

Sawdah Bhalmiya and Beatrice Nolan Mar 15, 2023, 4:53 PM GMT+9

IT & Networks

### AI tools like ChatGPT likely to empower hacks, NSA cyber boss warns

By **Colin Demarest** Thursday, Apr 13

digitaltrends.com

https://www.digitaltrends.com > Computing > News

### Great, hackers are now using ChatGPT to generate malware

2023. 2. 9. — A new threat has surfaced in the ChatGPT saga, with cybercriminals having developed a way to hack the AI chatbot and inundate it with ...

NEWSIS

### [단독]"해커의 모니터에 노트북 앞 기자 영상이"... 챗GPT 해킹 시연했더니

입력 2023.04.05. 오전 10:37 · 수정 2023.04.05. 오전 10:40

CNBC

TECH

### Microsoft introduces an A.I. chatbot for cybersecurity experts

PUBLISHED TUE, MAR 28 2023-11:30 AM EDT

Jordan Novet @JORDANNOVET

Alert on compromised account and device on Contoso.com

OneNote WMI PowerShell AMSI Kinsing Multisc Sabuk Wacatic

Summary Pinned items (5)

#### Alert Summary

This alert indicates that a device belonging to Devon Torres, a user of the contoso.com domain, was targeted by an emerging, financially motivated activity group that uses OneNote attachments to deliver remote access malware. The alert provides details about the suspicious process (ONNOTE.EXE) that was launched from a downloaded file (SalesLeads (1).onepkg) and its parent process (explorer.exe), as well as the device's hostname (workstation8), OS version (Windows 21H2), and risk score (High). The alert also shows the device's last seen time, external and internal IP addresses, and arrival status. The device has a user-defined tag (ContosoDemo) and is onboarded to Microsoft Defender for Endpoint (MDATP).

#### Attack Steps

The account dtorres@contoso.com was involved in a series of suspicious actions on the workstation8 host, indicating a possible compromise by a malware campaign.

#### The following attack steps were observed:

- Malicious OneNote package file downloaded
- Malicious scripts executed via WScript.exe
- Attempted AMSI tampering and process injection
- Suspicious Microsoft Defender Antivirus exclusion and startup folder addition
- Suspicious LDAP query and process discovery
- Suspicious WMI process creation
- Suspicious PowerShell command line and script execution

#### Attack Details

Malicious OneNote package file downloaded

# 사이버보안 주요 이슈와 현황

## ◆ 주요 이슈 (2) 랜섬웨어

- 가상화폐를 통한 비즈니스 모델이 성립되면서 랜섬웨어가 주요한 위협으로 부각되었으며, 국가안보 차원에서 대응해야 하는 수준으로 부상하고 있음

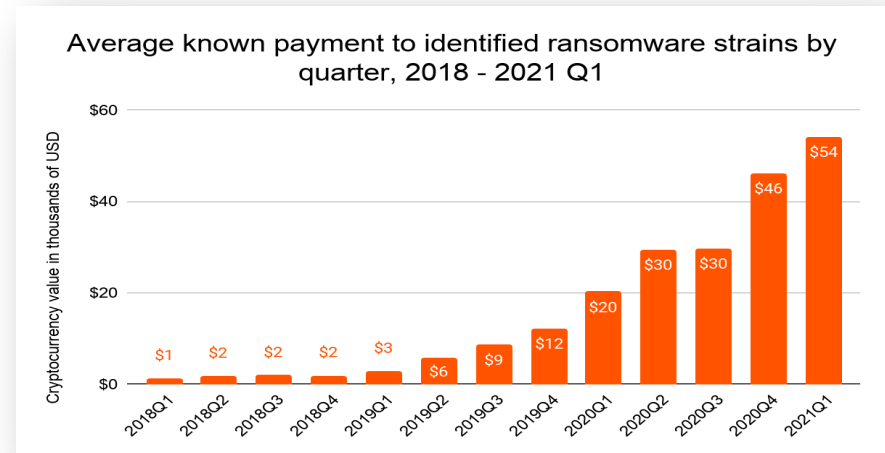
**The New York Times**

### White House Warns Companies to Act Now on Ransomware Defenses

An open letter urged them to take many of the defensive steps that the federal government requires of its agencies and contractors.

By **David E. Sanger** and **Nicole Perlroth**

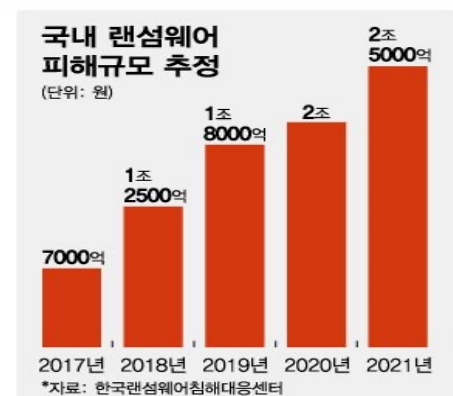
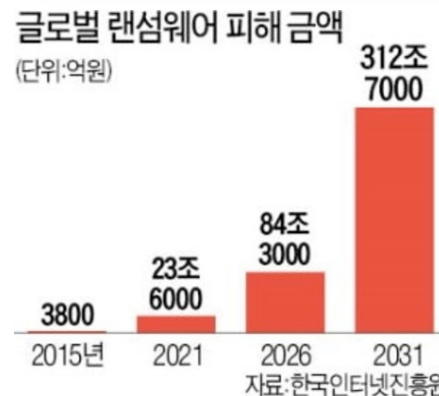
Published June 3, 2021 Updated Sept. 7, 2021



NOVEMBER 01, 2022

## International Counter Ransomware Initiative 2022 Joint Statement

BRIEFING ROOM STATEMENTS AND RELEASES



# 사이버보안 주요 이슈와 현황

## ◆ 주요 이슈 (3) 디지털자산과 자금세탁

- 가상화폐, NFT 등 디지털자산 시장의 확대로 이를 위협하는 사이버 위협이 증가하고 있음
  - '엑시 인피니티' 게임의 이더리움 서브체인 가상화폐 '로닌' 해킹으로 가상화폐 6억 달러 유출
  - 디파이 서비스의 스마트컨트랙트에 사용되는 토큰 취약점을 이용한 해킹이 발생해 Lendf.me의 2500만 달러 암호화폐와 UniSwap의 23만 달러의 암호화폐가 유출되는 사고 발생
- 북한은 디지털자산 탈취에 가장 적극적인 국가로 2022년 암호화폐 탈취 사건의 60%에 관여해 10억 불 이상을 탈취했으며 이 자금은 무기 개발에 사용된 것으로 추정됨
- 디지털자산을 활용한 자금세탁방지(ALM) 이슈가 주요 글로벌 이슈로 부각

연합뉴스 + 구독

### 미국토안보장관 "北, 암호화폐 등 10억불 이상 탈취해 무기개발"

입력 2022.10.19. 오전 8:18 기사원문

(서울=연합뉴스) 이상현 기자 = 북한이 지난 2년간 10억 달러(한화 1조4천억여원) 이상의 암호화폐 등을 탈취해 무기 개발에 사용했다고 알레한드로 마요르카스 미국 국토안보부 장관이 밝혔다.

마요르카스 장관은 18일 '싱가포르 국제 사이버주간 서밋'(SICWS) 행사 연설에서 "북한이 지난 2년 동안에 만 10억 달러가 넘는 암호화폐와 경화(hard currency)의 사이버 탈취를 통해 대량살상무기 프로그램에 자금을 지원했다"고 말했다고 미국의소리(VOA) 방송이 19일 보도했다.

INSIDER Jul 30, 2022

### Stolen money from cyberattacks makes up a third of the funds for North Korea's missile program, US official says

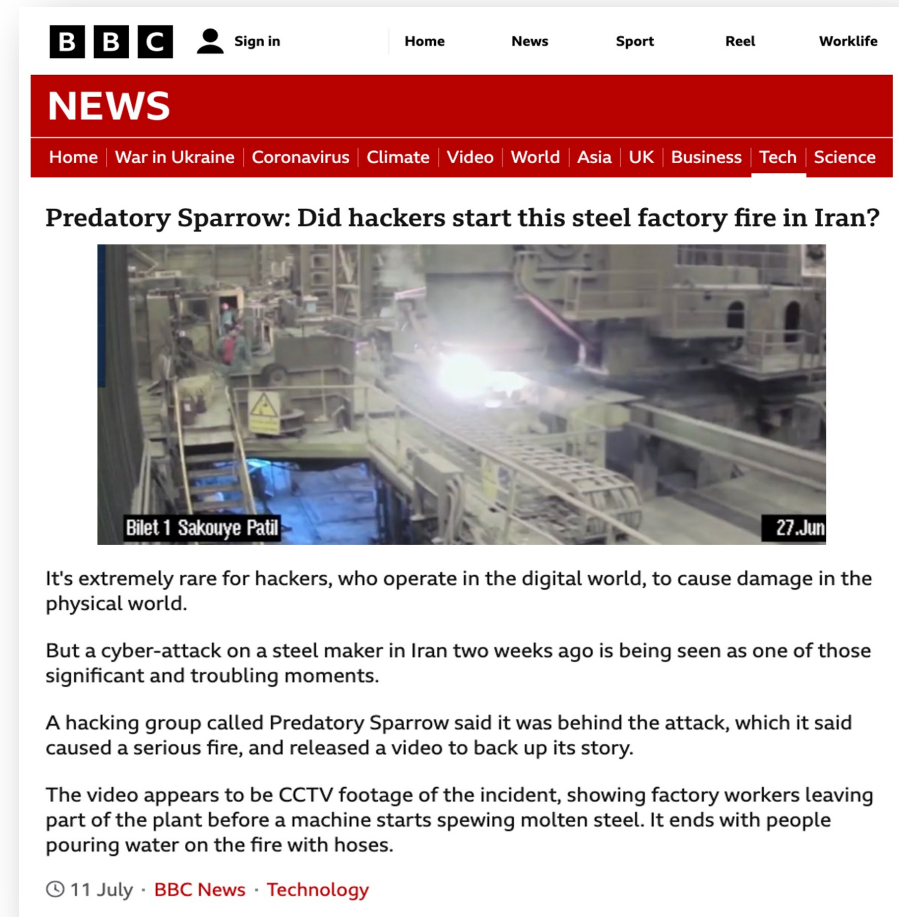
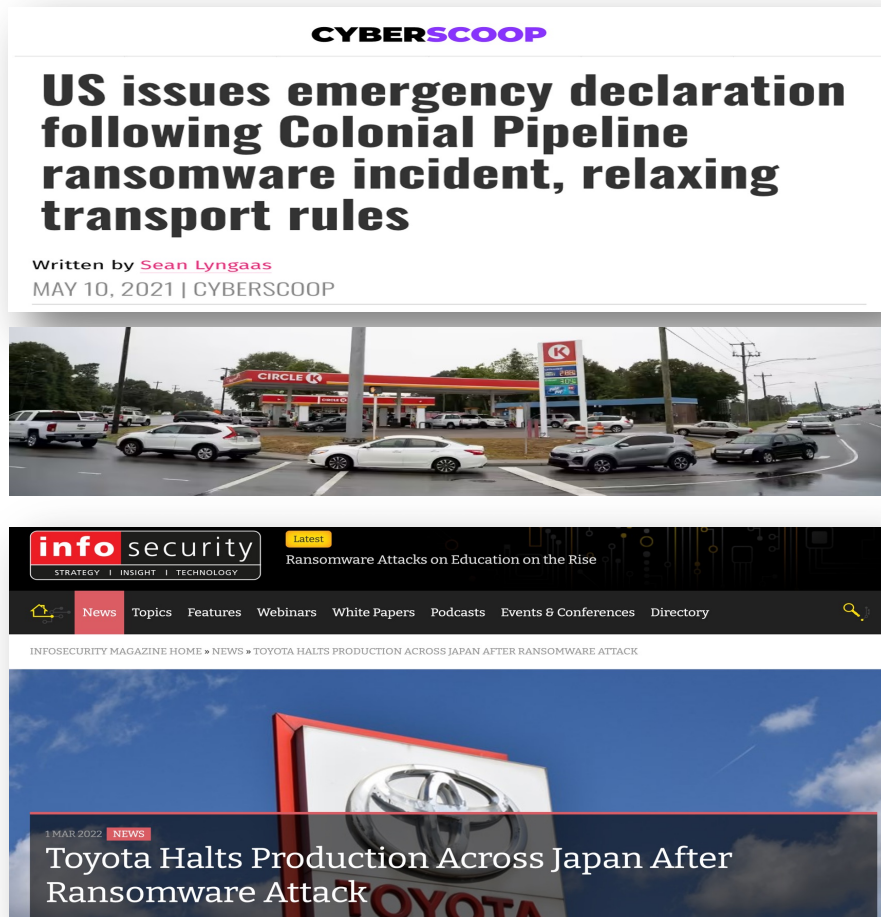


- One third of North Korea's missile program is funded by the country's cyberattacks.
- A US official said cyberattacks are a "core driver" of North Korea's revenue and have become a major concern.
- A 2022 UN report says that North Korean hackers walked away with more than \$400 million in cryptocurrency during cyberattacks in 2021.

# 사이버보안 주요 이슈와 현황

## ◆ 주요 이슈 (4) 기반시설·생산시설 대상 위협

- 콜로니얼 파이프라인 사례와 같이 사이버공격을 통해 기반시설·생산시설에 대한 위협이 가능하며, 최근에는 사이버공격으로 공장에 화재를 발생시켰다고 주장하는 사례도 발생





# 사이버보안 주요 이슈와 현황

## ◆ 주요 이슈 (5) 공급망 보안과 경제 안보

### ■ 공급망 통한 보안 위협 침투, 안전한 공급망

- 미 연방정부에서 사용하는 SolarWinds 프로그램 취약점을 통해 해커가 침투해 정부 기밀 유출
- 육군의 '해·강안과학경계사업' 일환으로 도입한 215개의 CCTV 조사 결과, 내부에 악성코드 유포로 활용되는 중국 IP가 입력되어 있어 보안 위협 문제 제기
- 5G 네트워크와 화웨이 장비 보안 논란과 같이 안전한 공급망 확보는 4차산업혁명의 필수 과제

### ■ 국가의 경제 안보 차원에서도 사이버안보 대응 필요

- 디지털경제의 비중이 증가하고 있는 상황에서 사이버공간의 안정성 확립 필요
- 신기술과 신기술들이 촉발하는 사회 변화에서 사이버안보 확립은 주요한 과제

연합뉴스 + 구독

#### 한미, 첫 경제안보대화...반도체협력-공급망 위기대응 강화 협의

입력 2022.07.07. 오후 10:24 기사원문

한국 측은 이 과정에서 미국이 주도하고 있는 과학기술 분야에 대한 협력 강화 필요성을 제기할 것으로 전망된다. 미국은 협력 강화 원칙에 더해 기술 보안 문제도 거론할 것으로 전망된다.

미국은 코로나19와 러시아의 우크라이나 침공 등으로 글로벌 공급망 위기가 발생하자 인도-태평양 경제 프레임워크(IPEF)를 출범시키는 등 동맹 및 파트너 국가 등을 위주로 경제 협력을 심화시키고 있다.

여기에는 안보적 측면에서 중국에 의존도를 줄이는 동시에 중국의 국제적 영향력을 차단하려는 대(對)중국 견제의 의미도 있다. 이와 관련, 미국은 중국의 사이버 해킹이나 첨단기술 절취 등도 심각하게 보고 대응하고 있다.

Forbes

CYBERSECURITY

#### Samsung Confirms Massive Galaxy Hack After 190GB Data Torrent Shared Via Telegram

Davey Winder Senior Contributor @  
Co-founder, Straight Talking Cyber

Follow

Mar 8, 2022, 04:50am EST

# 사이버보안 주요 이슈와 현황

## ◆ 주요 이슈 (6) 정보유출

- 북한은 군사기밀 및 방위산업체 보유 정보 등 외에도 기반시설 관련 정보, 연구, 의료정보 등 다양한 정보를 탈취하기 위해 사이버공격을 지속적으로 수행하고 있음

파이낸셜뉴스

### 방사청 "KFX·잠수함설계도 등 유출의심" 해킹 공격 급증

입력 2022.10.13. 오전 11:14

파이낸셜뉴스 (+) 구독

### 北공작원 지령 받고 군사기밀 유출..현역 장교·민간인 구속 기소

입력 2022.04.28. 오후 4:21 (기사원문)

TVCHOSUN (+) 구독

PICK ①

### [단독] 서울대병원 해킹도 北소행...유력인사 의료기록 유출 우려

입력 2021.07.14. 오후 9:39 - 수정 2021.07.14. 오후 9:45 (기사원문)

한국경제

### 연이은 韓 연구원 해킹에...美 "北, 악의적인 사이버 활동"

기사입력 2021-07-09 13:55

news 1 (+) 구독

### [단독] 주요 방산업체 상대 해킹시도, 최근 1년새 '121만 건'

입력 2021.10.12. 오전 9:14 - 수정 2021.10.12. 오전 9:15 (기사원문)

## 북한발 정보유출 목적의 해킹

- 2021년 원자력발전 관련 연구를 수행하는 원자력연구원, 도산안창호함을 비롯해 우리 주력 잠수함을 건조하는 방산업체 대우조선해양, KF-21 생산업체 KAI 등이 잇따라 북한 추정 해킹 공격을 당함
- 코로나19로 재택근무가 확산되면서 외부 업무를 위한 VPN 관련 취약점을 이용한 사이버공격이 급증했으며, 이번 공격들도 VPN 취약점을 통해 침투한 것으로 추정
- 서울대병원, 성모병원 등 의료정보에 대한 해킹, 국방부 자문위원단 등을 대상으로 국방 기밀 유출을 위한 해킹 시도 역시 지속적으로 발생하고 있는 상황

## 2. 사이버보안 패러다임의 변화

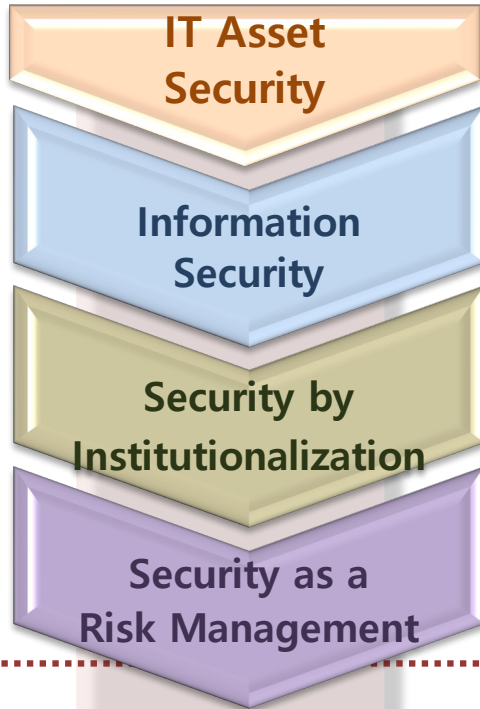
# 사이버보안 패러다임의 변화

## ◆ 사회 환경의 변화 : 정보화사회에서 초연결사회로의 전환

	정보사회	초연결사회
연결의 핵심요소	데이터, 커뮤니케이션	사물, 상태, 상황
연결의 구조	단선적, 병렬적 연계	다선적, 직렬적 연계
연결의 속성	네트워크 연결에 집중	연결 후 상호연계성에 집중
연결의 주요 가치	유동성, 도달성	일괄성, 관계성
연결의 구성	 <p>[사이버 공간] 데이터 커뮤니케이션 [물리적 공간]</p>	 <p>[사이버 공간] condition [물리적 공간] 사물</p>

# 사이버보안 패러다임의 변화

## ◆ 보안 패러다임의 전환



정보통신 기술들의 사용이 확산됨에 따라,  
물리 보안에서 IT 자산 보안(IT Asset Security)으로 변화

정보화시대의 도래로 개인정보보호, 지식재산권 보호 등  
'정보' 중심의 보안 패러다임인 정보보호로 변화

기업 업무 환경에서 IT 비중이 높아지면서 제도적으로 보안을 규정하거나  
인증제도를 통하여 기술적·관리적 보호조치를 갖추도록 하며  
제도에 대한 준수(Compliance)가 중심이 됨

조직 전사적 위험관리(ERM) 차원에서 보안을 고려하여  
내부통제, 보안거버넌스, 통합적 보안(Holistic Security)을 강조

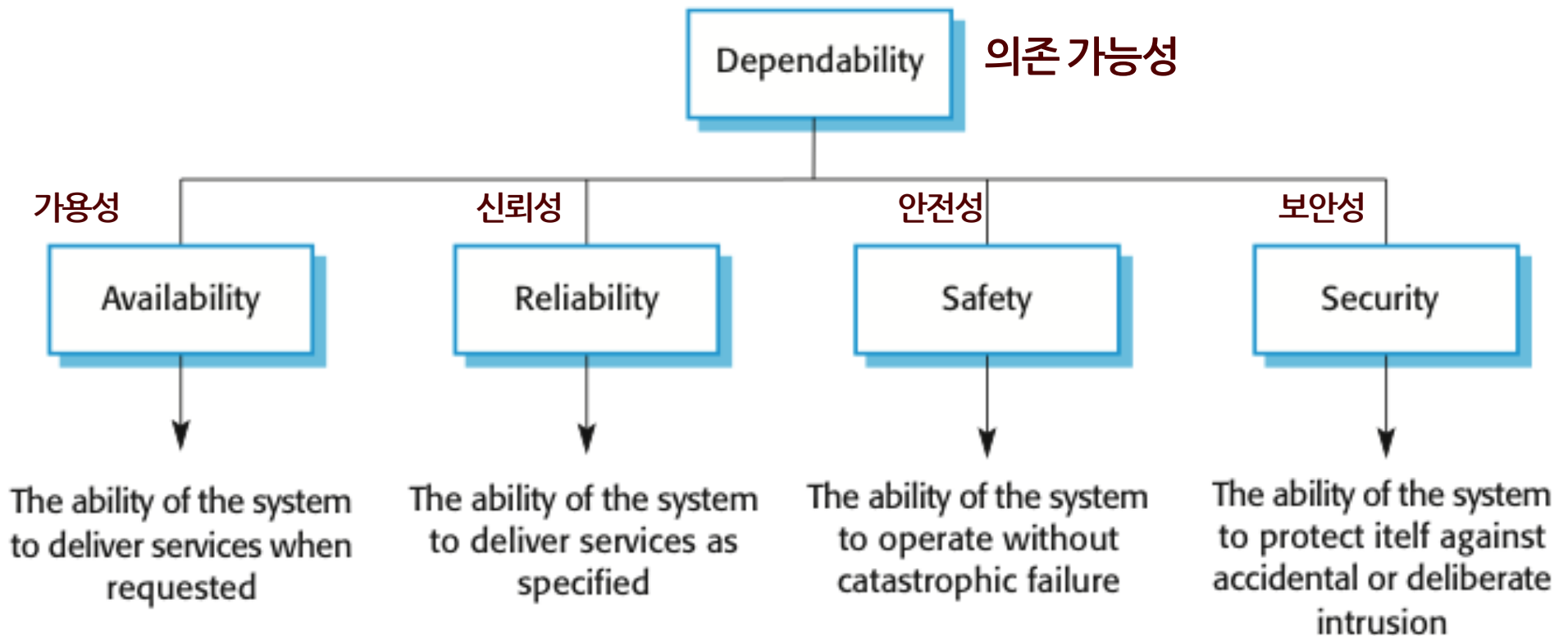
사이버 위협 고도화 및 증가, 사이버인프라의 복잡성 증대 등에 따라  
사전적 방어 중심의 보안에서 언제든지 공격을 받을 수 있으며  
신속히 대처하고 정상화하는 '회복탄력성(Resilience)' 중요성 강조

사이버물리시스템과 같이 전통적인 분야에도 ICT가 결합되면서  
전통적인 보안 외에도 안전성, 신뢰성, 관리가능성 등을 포괄하는  
시스템에 대한 '의존 가능성(Dependability)'이 등장

# 사이버보안 패러다임의 변화 - 의존 가능성

## ◆ 사이버보안과 Dependability(의존 가능성)

- '의존 가능성'은 보안을 포괄하여 시스템의 신뢰성, 가용성, 안전성 등을 모두 고려하는 개념으로 물리적인 위협과 결부되는 CPS(사이버물리시스템) 환경에서 특히 강조되고 있음



J. C. Laprie, A. Costes: "Dependability: A unifying concept for reliable computing", 12th IEEE International Symposium on Fault-Tolerant Computing(FTCS-12), 1982

# 사이버보안 패러다임의 변화 - 레질리언스

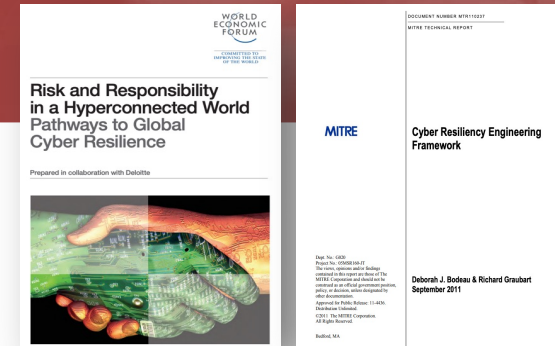
## ◆ 사이버 레질리언스의 개념

### ■ 사이버 레질리언스 관련 주요 정의

- 환경 변화에 적용하는 능력이며 방해로부터 준비되고 견디며, 빠르게 복구할 수 있는 능력으로 시스템, 인프라 등에 적용 가능 (DHS Risk Lexicon, 2010)
- 국가, 조직 또는 임무 또는 비즈니스 프로세스가 기능을 수행하는 데 필요한 지원 사이버 리소스에 대한 불리한 조건, 스트레스 또는 공격에 직면하여 기능을 개선하기 위해 예측, 저항, 복구 및 진화하는 능력 (MITRE, 2011)
- 평균 실패 시간과 평균 복구 시간의 조합으로 측정되는 사이버 공격에 견딜 수 있는 시스템 및 조직의 능력 (World Economic Forum, 2012)
- 사이버 자원을 사용하거나 이로 구현되는 시스템에 대한 악의적 조건, 공격, 압박, 침해 등을 예상하고 견디고 복구하고 적응하는 능력 (NIST SP 800-160 Vol.2., 2019)

### ■ 다양한 정의들을 조합하여 사이버보안 레질리언스에 대한 정의

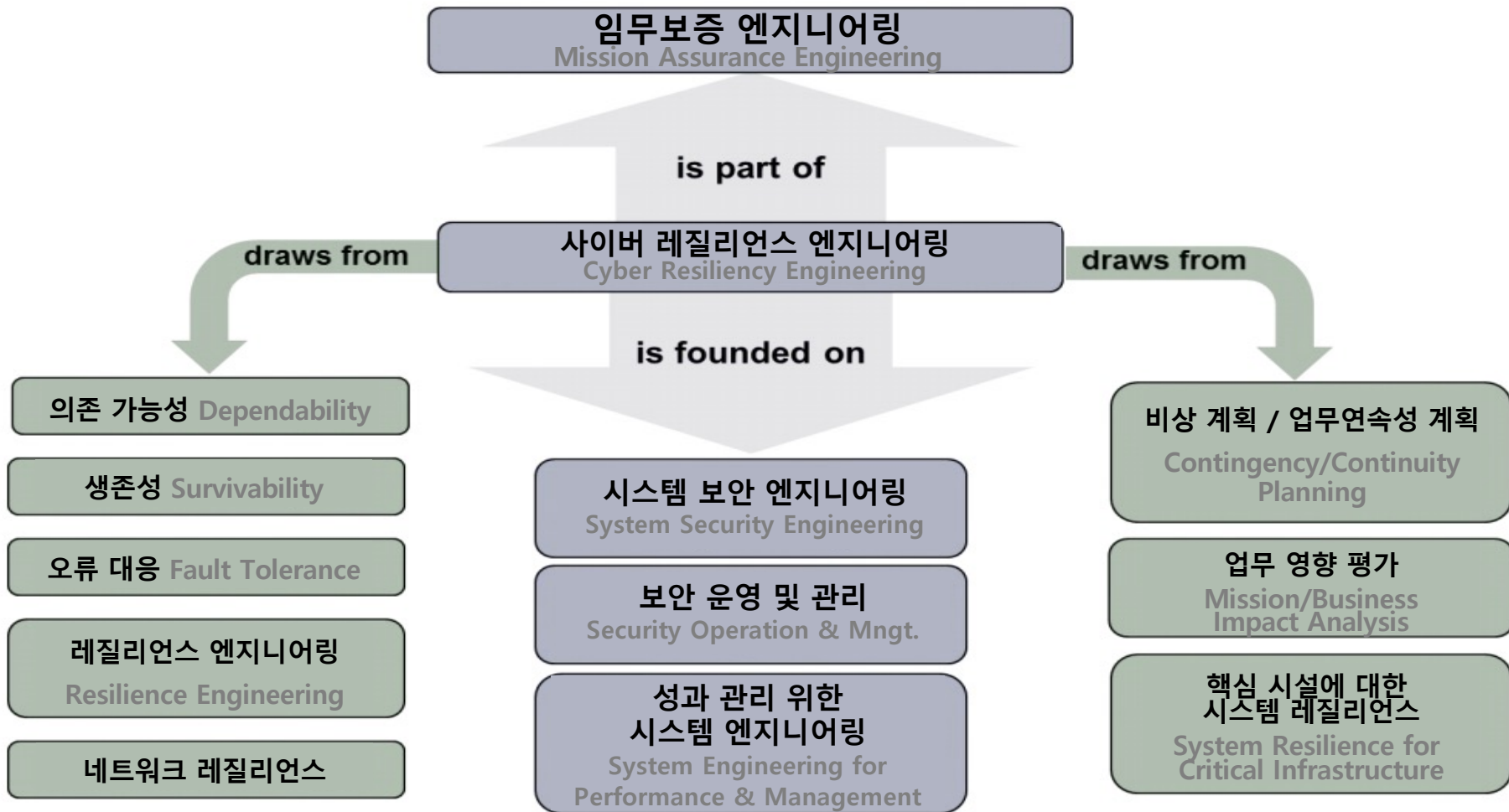
- 사이버인프라가 다양한 내외부적 위협으로부터 대비하고, 견디고, 복구 및 적응할 수 있는 능력을 의미
  - 대비(Prepare), 견딤(Withstand), 복구(Recover), 적응/진화(Evolve) 등의 개념이 공통적으로 활용



# 사이버보안 패러다임의 변화 - 레질리언스

## ◆ 사이버 레질리언스 구현

- 사이버 레질리언스 엔지니어링과 기존 보안 활동과의 관계





# 사이버보안 패러다임의 변화 - 레질리언스

## ◆ 사이버 레질리언스 구현

### ■ 사이버 레질리언스 기술적 구현적 접근법

<p><b>맞춤형 대응</b></p> <p>동적 재구성 동적 리소스 할당 적응형 관리</p>	<p><b>분석 모니터링</b></p> <p>모니터링 및 손상 평가 센서 융합 분석 포렌식 및 행동분석</p>	<p><b>협력 기반 보호</b></p> <p>보정된 심층 방호 일관성 분석 협업 자기 도전</p>	<p><b>상황 인식</b></p> <p>동적 리소스 인식 동적 위협 인식 임무 종속성 및 상황 시각화</p>	<p><b>(적) 기만 행위</b></p> <p>혼란 유발 가짜 정보 오인 유도 오염</p>	<p><b>다각화</b></p> <p>설계 다각화 구문 다각화 정보 다각화 경로 다각화 공급망 다각화</p>	<p><b>동적 포니셔닝</b></p> <p>센서 기능 기반재배치 자원 기능 최적화 자산 이동성 다각화 기능 분산화</p>
<p><b>비지속성</b></p> <p>비지속적 정보 비지속적 서비스 비지속적 연결</p>	<p><b>권한 제한</b></p> <p>신뢰 기반 권한 관리 속성 기반 사용 제한 동적 권한</p>	<p><b>재정렬</b></p> <p>목적기반 비필수적 요소 탑재 제거 제한 대치 전문화</p>	<p><b>이중(중복)화</b></p> <p>보호된 백업 및 복원 비상용 자원 복제</p>	<p><b>격리</b></p> <p>사전 설계 기반 격리 동적 분할 및 격리</p>	<p><b>무결성 입증</b></p> <p>무결성 검증 출처 추적 행동 검증</p>	<p><b>예측 불가능성</b></p> <p>(무작위적) 일시적 예측 불가능 (사전 계획된) 상황적 예측 불가능성</p>

### 3. 대한민국 사이버안보 확립 방안

# 대한민국 사이버안보 확립 방안

## ◆ 윤석열정부의 101번째 국정과제, 사이버안보

### ■ 국정과제의 101번째 국정과제로 사이버안보 포함

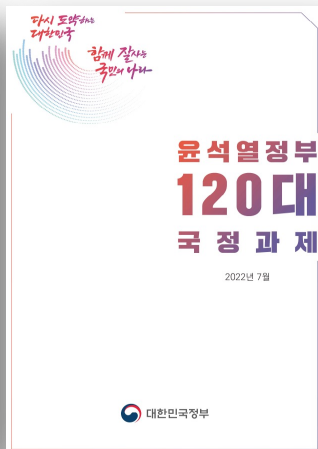
- 국정과제에 사이버안보 확립을 위한 국가 사이버안보 대응 역량 강화 선정
- '국정목표 5. 자유, 평화, 번영에 기여하는 글로벌 중추국가' 등 외교·안보의 과제로 식별

### ■ 국가 사이버안보 대응 역량 강화 방안

- '국가사이버안보위원회' 신설과 컨트롤타워, 부처별 역할과 책임 등 거버넌스 체계 확립
- 민관 협력, 디지털 플랫폼 정부 보안, 신기술 개발 등 경제안보 관점의 대응
- 사이버 전문인력 양성 강화, 사이버예비군 신설 등 사이버안보의 핵심인 인력 양성 및 강화

## 윤석열정부 110대 국정과제

2022년 5월



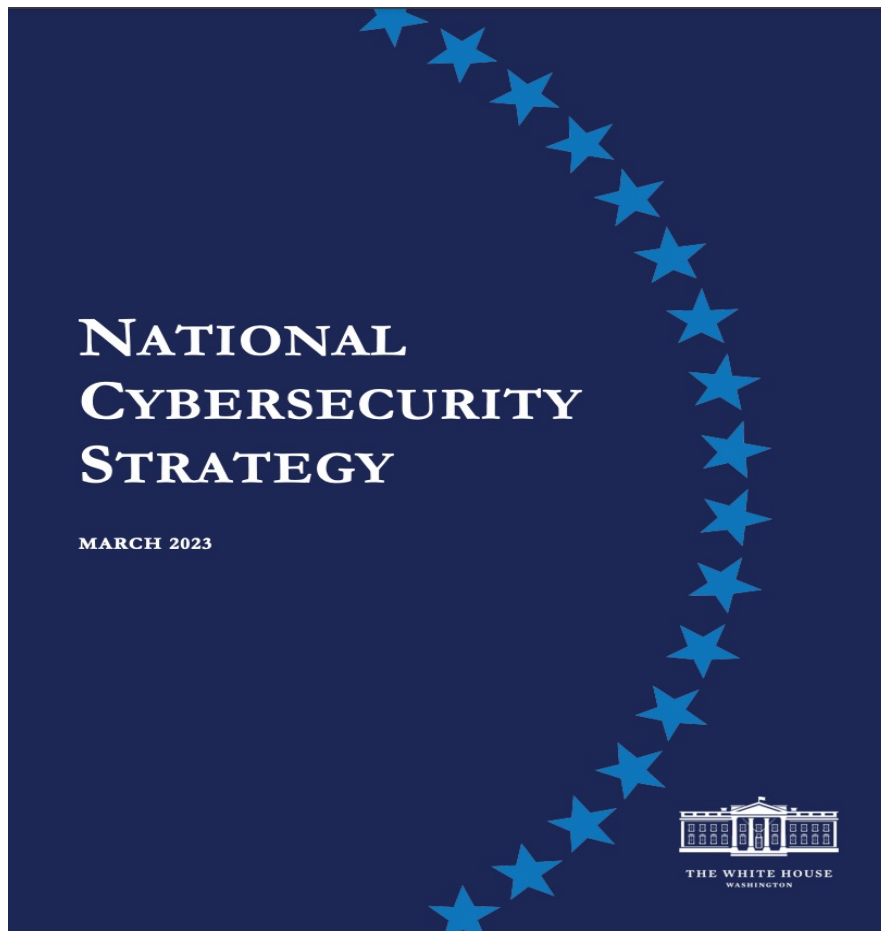
## 101 국가 사이버안보 대응역량 강화 (국정원·과기정통부·국방부·외교부)

### □ 과제목표

- 전통적 국가안보 영역에서 경제안보·국민생활까지 확장 추세인 국가배후 조직 및 국제 해킹조직의 위협에 대응하는 **사이버안보 패러다임 구축**
- **汎정부 차원 협력체계 공고화**, 사이버 방어체계 및 국제공조 시스템 강화를 통해 확고한 국가안보 태세 유지 및 국민·기업에 안전한 사이버환경 제공
- 관련 산업·기술 경쟁력 제고, 인재 육성 등을 통해 **사이버안보 기반 공고화**

## ◆ 미 바이든 행정부의 사이버안보 확립을 위한 노력

- 바이든 행정부는 2023년 3월, 최초로 발간한 국가안보전략에서 중국과 경쟁을 위한 전략을 제시하며, 사이버안보 역시 주요 요소로 제시함



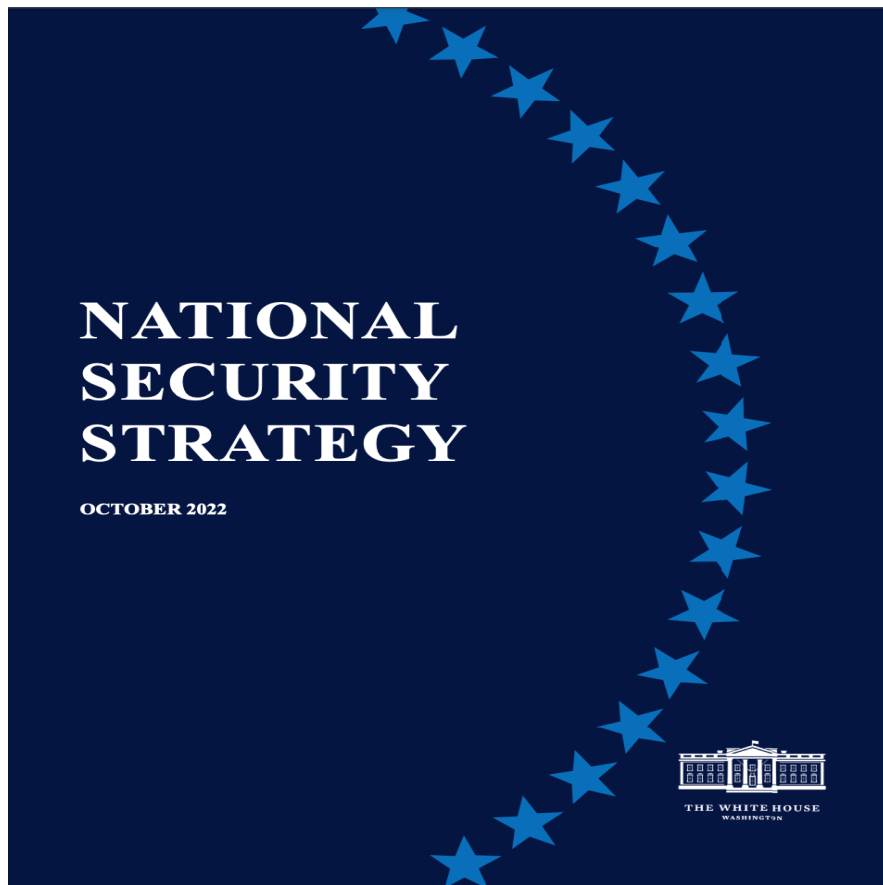
### 바이든 행정부 '국가사이버안보전략'

- 사이버안보 비전으로 Defensible, Resilient, Values-aligned를 천명
- 국가 사이버안보 확립을 위해 (1)주요 인프라 보호 (2)위협 행위자 방해 및 해체, (3)보안과 레질리언스 추진 위한 시장 힘 형성, (4)회복 가능한 미래를 위한 투자, (5)공동의 목표 추구 위한 글로벌 파트너십 구축 등 5개의 Pillar를 통해 국가 사이버보안 확립 방안을 제시함
- (1) 책임과 규제 재분배 등 기업 대상 책임 부과 기조 (2) 억지(deterrence)라는 기존 사이버안보 접근법이 언급되지 않음, (3) 위협 행위 대응 위한 군사력 사용 등 적극적 기조 등 기존 전략 대비 변화 확인 가능

# 대한민국 사이버안보 확립 방안 - 미국의 사례

## ◆ 미 바이든 행정부의 사이버안보 확립을 위한 노력

- 바이든 행정부는 2022년 10월, 최초로 발간한 국가안보전략에서 중국과 경쟁을 위한 전략을 제시하며, 사이버안보 역시 주요 요소로 제시함



### 미국의 '국가안보 전략'

- 미국은 골드워터-니콜스법에 따라 대통령의 '국가안보전략' 의회 제출 의무화
- 부시행정부 : 2002년 9월 '선제적 전쟁 (preemptive war)' 기초, 2006년 3월 '폭정의 종식(ending tyranny)' 기초의 NSS 발간
- 오바마 행정부 : 2010년 3월, '국내 역량 강화와 이를 통한 국제 질서 형성 (building at home, shaping abroad)' 기초, 2015년 1월, '전략적 인내 (strategic patience)' 기초의 NSS 발간
- 트럼프 행정부 : 2017년 12월, '미국 우선주의 (America first)' 기초의 NSS 발간
- 바이든 행정부 : 2022년 10월, '전략적 경쟁 (strategic competition)' 기초의 NSS 발간

# 대한민국 사이버안보 확립 방안 - 미국의 사례

## ◆ 미국의 국가 사이버안보 확립을 위한 노력

- 2019년 국방수권법안에 따라 창설된 '사이버공간 솔라리움 위원회'는 2020년 3월, 사이버 역지력 확립을 위한 종합 전략을 제시했으며, 바이든 정부에서도 이를 계승하여 진행중

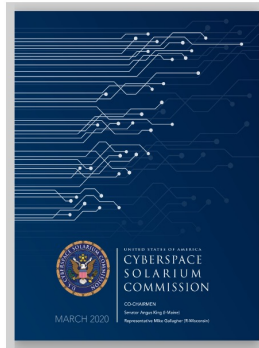


### Introduction

The Cyberspace Solarium Commission (CSC) was [established](#) in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The finished report was presented to the public on March 11, 2020. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 [reauthorized](#) the Commission to collect and assess feedback on the analysis and recommendations contained within the final report, review the implementation of the recommendations contained within the final report, and completing the activities originally set forth for the Commission.

### Our Report

The Cyberspace Solarium Commission's proposes a strategy of layered cyber deterrence. Our report consists of over 80 recommendations to implement the strategy. These recommendations are organized into 6 pillars:



## 사이버 솔라리움 위원회 권고안

- 2019년 국방수권법안의 요구에 따라 사이버 공간에서 미국의 국익을 보호하기 위해 냉전 시대 소련 위협에 대응하기 위해 운영되었던 솔라리움을 차용한 사이버솔라리움위원회 창설
- 2020년 3월, 사이버솔라리움위원회는 사이버 안보 강화를 위해 1개의 기반, 3개의 레이어 6가지 Pillar에 따른 82개의 권고안을 제시함
  1. 사이버 대응을 위한 미 정부의 구조 및 조직 개혁
  2. 사이버공간에서 책임 있는 행동 장려를 위한 규범과 비군사적 도구 강화
  3. 미국의 사이버 위협에 대한 레질리언스 강화
  4. 미국의 사이버보안 강화를 위한 사이버 생태계 재구성
  5. 민간과의 사이버보안 협력 강화
  6. 악의적 활동에 책임 부과 위한 군사력 유지 및 활용

# 대한민국 사이버안보 확립 방안 - 미국의 사례

## ◆ 미국의 국가 사이버안보 확립을 위한 노력

- 트럼프 행정부에서 '전진 방호(Defend Forward)'와 '지속적 개입(Persistent Engagement)'의 사이버국방 전략을 채택했으며, 이는 '통합적 억지(Integrated Deterrence)'로 계승



U.S. CYBER COMMAND

Home About FOIA/Privacy Act Media Partnerships and Outreach Employment Opportunities COVID-19

NEWS | Oct. 25, 2022

### CYBER101 - Defend Forward and Persistent Engagement

By U.S. Cyber Command PAO U.S. Cyber Command

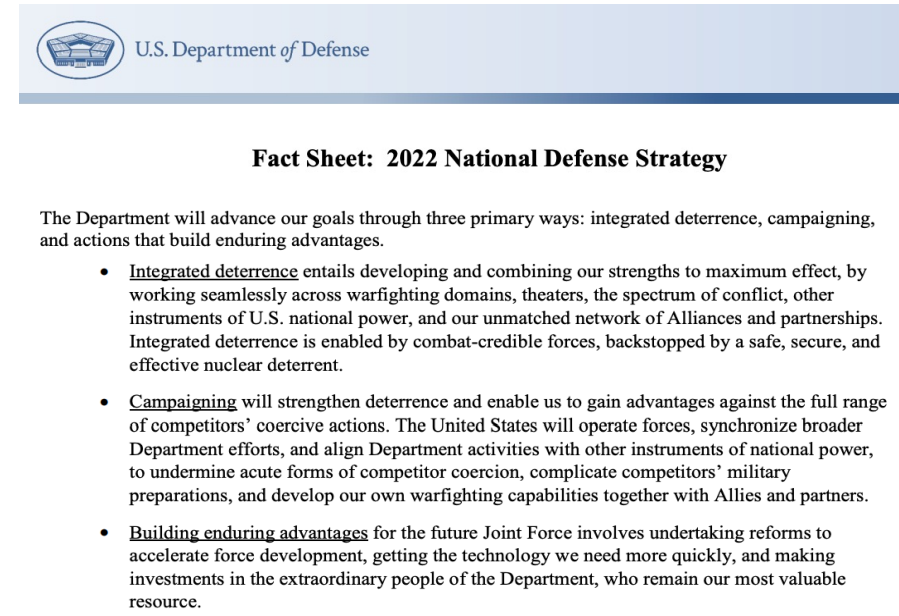
Fort George G. Meade, Maryland – Cyberspace is not governed by a central body, but by numerous government and non-governmental organizations across the globe. The cyber domain is not naturally occurring and is wholly dependent upon owned or leased technology on both government and commercial infrastructure providers for its existence and operation. Due to the ever-evolving technological aspects of the information environment, adversaries are continuously looking to disrupt and degrade the integrity of U.S. information networks and those of its allies and partners.



U.S. Department of Defense

### 'Persistent Engagement' Strategy Paying Dividends, Cybercom General Says

Nov. 10, 2021 | By [David Vergun](#), DOD News | [f](#) [t](#) [r](#)



U.S. Department of Defense

### Fact Sheet: 2022 National Defense Strategy

The Department will advance our goals through three primary ways: integrated deterrence, campaigning, and actions that build enduring advantages.

- **Integrated deterrence** entails developing and combining our strengths to maximum effect, by working seamlessly across warfighting domains, theaters, the spectrum of conflict, other instruments of U.S. national power, and our unmatched network of Alliances and partnerships. Integrated deterrence is enabled by combat-credible forces, backstopped by a safe, secure, and effective nuclear deterrent.
- **Campaigning** will strengthen deterrence and enable us to gain advantages against the full range of competitors' coercive actions. The United States will operate forces, synchronize broader Department efforts, and align Department activities with other instruments of national power, to undermine acute forms of competitor coercion, complicate competitors' military preparations, and develop our own warfighting capabilities together with Allies and partners.
- **Building enduring advantages** for the future Joint Force involves undertaking reforms to accelerate force development, getting the technology we need more quickly, and making investments in the extraordinary people of the Department, who remain our most valuable resource.



U.S. Department of Defense

### Official Says Integrated Deterrence Key to National Defense Strategy

Dec. 6, 2022 | By [David Vergun](#), DOD News

# 대한민국 사이버안보 확립 방안

## ◆ 제언 : 대한민국 사이버안보 확립 방안

### ■ 1. 사이버안보 법 체계 정비

- 민·관·군 분절된 대응 체계에서 국가역량을 결집할 수 있는 체계로 전환
- 사이버안보(보안) 관련 기본법을 통해 사이버안보 컨트롤타워로 국가안보실을 명확히 규정하며, 각 부처의 역할을 정립하고 위기 시 국가역량을 결집할 수 있는 근거를 만들 필요

### ■ 2. 능동적/선제적 사이버안보 패러다임 확립

- 진화하는 사이버 위협 대응 위한 능동적/선제적 대응 기조 포괄 국가사이버안보전략 수립
- 공세적 작전을 고려한 전략 수립과 이를 뒷받침 할 수 있는 작전 수행 역량 확보
- 양자간·다자간 국제협력을 통해 보다 실효적인 악의적 주체 제재 방안 마련

### ■ 3. 민·관 사이버안보 협력 강화

- 정부가 지원하고 민간이 주도하는 사이버안보 기술의 '전략산업화' 추진
- 신설되는 '사이버안보협력센터' 통한 민·관 정보공유범국가적 사이버위협 대응 기반 구축

### ■ 4. 레질리언스 확립

- 레질리언스 중심의 사이버보안 패러다임으로 전환하여 위협 상황 대응력 강화



## 4. 결론 및 시사점

# 결론 및 시사점

## ◆ 국가안보의 모든 영역에서 사이버안보에 대한 중요성이 부각되고 있음

- 사이버공간의 제4, 제5 전장화
- 국가차원의 사이버위협 대응

- 국가기반시설 사회 안전
- CPS 환경에서 국민 안전 위협

- 선거 개입 : 심리전, 가짜뉴스
- 체재 위협 : 색깔혁명

- 국가 간 분쟁에서 사이버 이슈 해결
- 국제법, 국제 협력 활동 참여 필요

- 사이버 방첩, 첩보 활동 강화 필요
- 국내 사이버 첩보 활동에서 프라이버시와 균형점 확보

- 사이버공간에서의 범죄행위 대응
- 사법 공조, 수사 역량 강화 등

- 인터넷 기반 산업 보호
- 산업기밀 등 지식재산권 탈취 대응

- 5G 등 차세대 인프라 보안
- 신기술에서의 기술 우위와 보안, 프라이버시 확보



# 결론 및 시사점

## ◆ 사이버안보 확립의 필요성



사이버안보 확립은 대한민국 안보와 국익 보호를 위하여 핵심적인 과제

# 결론 및 시사점

## ◆ 전문인력의 중요성

- 글로벌 주요 싱크탱크들은 일찍이 사이버보안 전문인력의 양성 필요성 강조

### A Human Capital Crisis in Cybersecurity

Technical Proficiency Matters

A Report of the  
CSIS Commission on Cybersecurity for the 44th Presidency

## H4CKER5 WANTED

An Examination of the Cybersecurity Labor Market



MARTIN C. LIBICKI  
DAVID SENTRY  
JULIA POLLAK

### 사이버보안 전문인력의 중요성

- CSIS는 2010년 오바마 대통령 취임 시 발간한 '44대 대통령을 위한 사이버보안 제언'에서 전문인력 양성의 중요성을 강조했으며, 특히 인력 부족에 따른 국가 위기 가능성을 경고함
- 랜드연구소 역시 2014년 'H4CKER5 Wanted' 라는 보고서를 통해 국가 차원에서 해커 등 사이버안보 전문가 확보의 필요성 강조
- 사이버안보는 고급 해킹 기술과 상상력을 가진 공격자와 이를 방어하는 전문 방어 역량 간의 대결로 결국 사람 간의 두뇌 전쟁
- ChatGPT, DARPA의 Cyber Grand Challenge, 같이 A.I.에 의하여 해킹과 보안 인력이 대체 될 수 있는 상황에서 고급인력 양성 필요

## ◆ 전문인력의 중요성

- 미 바이든행정부와 트럼프행정부에서도 국가의 전략자산으로서 전문인력 육성 추진

EXECUTIVE ORDERS

### Executive Order on America's Cybersecurity Workforce

ECONOMY & JOBS | Issued on: May 2, 2019

Section 1. Policy. (a) America's cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. The National Cyber Strategy, the President's 2018 Management Agenda, and Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and

BRIEFING ROOM

### FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity

AUGUST 25, 2021 • STATEMENTS AND RELEASES



**Biden administration establishes program to recruit tech professionals to serve in government**

Just In...

BY MAGGIE MILLER - 08/30/21 05:48 PM EDT

103

## 사이버보안 전문인력에 대한 강조

- 트럼프 행정부와 바이든 행정부는 모두 사이버보안에서 인력의 중요성을 강조했으며, 사이버보안 전문인력 확보를 위한 정책을 추진함
- 트럼프 행정부는 사이버보안 전문인력을 미국의 전략 자산이라 인식하고 재능을 갖춘 인재(Talents) 확보 방안과 재능을 보상하며 정부가 이들을 확보하는 방안, 재능 있는 인재를 육성하는 교육에 대한 인센티브 부여 방안 등을 요구함
- 바이든 행정부는 여러 행정명령과 정책을 통해 사이버보안 강화와 이를 위한 인력 양성과 확보를 강조했으며, 최근 사이버보안을 위한 간담회에서도 IBM, 텍사스 대학 등에서는 인력 관련 대안을 논의함

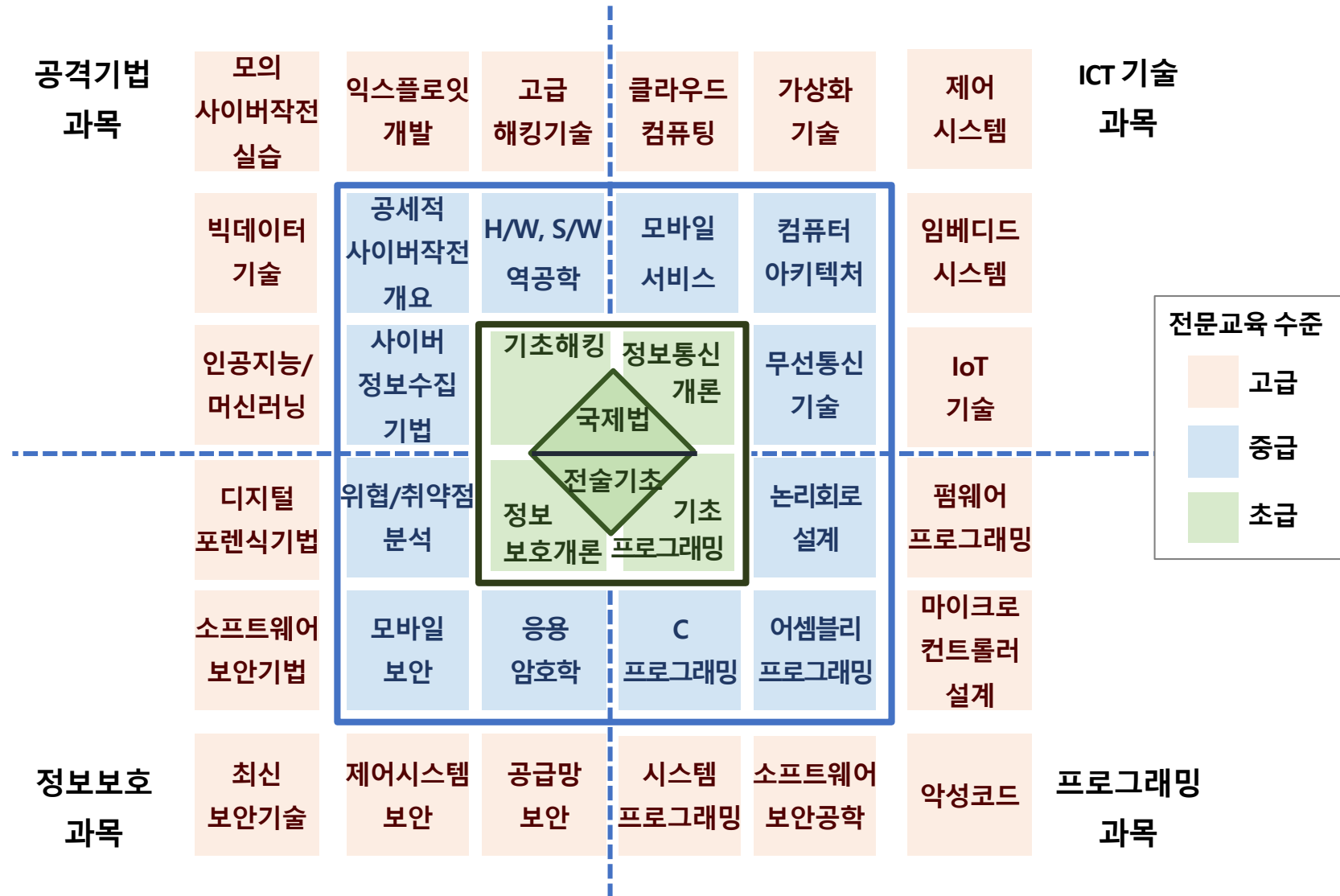
# 결론 및 시사점

## ◆ 전문인력의 역량 - 사이버방호



# 결론 및 시사점

## ◆ 전문인력의 역량 - 사이버작전



**감사합니다.**

**[jilim76@gmail.com](mailto:jilim76@gmail.com)**